

APPENDICES

LIST OF ACRONYMS

ACS – Automated Case Support System
ADIC – Assistant Director in Charge
AG Guidelines – Attorney General Guidelines
AGRT – Attorney General’s Review Team
ALAT – Assistant Legal Attache
ASAC – Assistant Special Agent in Charge
AUSA – Assistant United States Attorney

CDC – Chief Division Counsel
CIA – Central Intelligence Agency
CIR – Central Intelligence Report (CIA)
CIRG – Critical Incidents Response Group
CTC – Counter Terrorist Center (CIA)
CTD – Counterterrorism Division (FBI)

DCI – Director of Central Intelligence
DEA – Drug Enforcement Administration
DTOS – Domestic Terrorism Operations Section

EC – Electronic Communication

FAA – Federal Aviation Administration
FBI – Federal Bureau of Investigation
FCI – Foreign Counterintelligence
FFI – Full Field Investigation
FISA – Foreign Intelligence Surveillance Act
FISC – Foreign Intelligence Surveillance Court
FTO – Foreign Terrorist Organization

GAO – General Accounting Office

IIIA – Integrated Intelligence Information Application
INS – Immigration and Naturalization Service
IOS – Intelligence Operations Specialist
IRS – Intelligence Research Specialist
ISD – Investigative Services Division

ITOS – International Terrorism Operations Section

JICI –Joint Intelligence Committee Inquiry

JTTF – Joint Terrorism Task Force

LEGAT – Legal Attache

LHM – Letterhead Memorandum

MAOP – Manual of Administrative Operations and Procedures

MIOG – Manual of Investigative Operations and Guidelines

NSA – National Security Agency

NDPO - National Domestic Preparedness Office

NIPC – National Infrastructure Protection Program

NFIP – National Foreign Intelligence Program

NSD – National Security Division

NSL – National Security Letter

NSLU – National Security Law Unit

OGC – Office of General Counsel

OIG – Office of the Inspector General

OIPR – Office of Intelligence Policy and Review

OLC – Office of Legal Counsel

OPR – Office of Professional Responsibility

ORCON – Originator controlled

PI – Preliminary Inquiry

RFU – Radical Fundamentalist Unit

SAC – Special Agent in Charge

SCI – Sensitive compartmented information

SCIF – Sensitive Compartmented Information Facility

SDNY – Southern District of New York

SIOC – Strategic Information & Operations Center

SSA – Supervisory Special Agent

STU III – Secure Telephone Unit third generation

TAOG – Threat Assessment Operations Group

TD – Telegraphic Dissemination (CIA)

TECS – Treasury Enforcement Communication System

UBL – Usama Bin Laden

UBLU – Usama Bin Laden Unit

USAO – United States Attorney's Office

USIC – U.S. Intelligence Community

WTC – World Trade Center

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 07/10/2001

To: Counterterrorism

Attn: RFU

SSA [REDACTED]

IRS [REDACTED]

UBL Unit

SSA [REDACTED]

IRS [REDACTED]

IRS [REDACTED]

IRS [REDACTED]

I-46

SSA [REDACTED]

SA [REDACTED]

PENT BOMB
INFORMATION CONCERNING

New York

From: Phoenix

Squad16

Contact: SA Kenneth J. Williams [REDACTED]

Approved By: [REDACTED]

Drafted By: Williams Kenneth J

Case ID #: [REDACTED] (Pending)

Title: [REDACTED]
IT-OTHER (ISLAMIC ARMY OF THE CAUCASUS)

Synopsis: [REDACTED] UBL and AL-MUHAJIROUN supporters attending civil aviation universities/colleges in the State of Arizona.

Derived From : G-3

Declassify On: X1

Full Field Investigation Instituted: 04/17/2000 (NONUSPER)

Details: [REDACTED] The purpose of this communication is to advise the Bureau and New York of the possibility of a coordinated effort by USAMA-BIN-LADEN (UBL) to send students to the United States to attend civil aviation universities and colleges. Phoenix has observed an inordinate number of individuals of investigative interest who are attending or who have attended civil aviation universities and colleges in the State of Arizona. The inordinate number of these individuals attending these type of schools and fatwas issued by AL-

000383 [REDACTED]

To: Counterterrorism From: Phoenix
Re: [REDACTED] 07/10/2001

MUHJIROUN spiritual leader SHEIKH OMAR BAKRI MOHAMMED FOSTOK, an ardent supporter of UBL, gives reason to believe that a coordinated effort is underway to establish a cadre of individuals who will one day be working in the civil aviation community around the world. These individuals will be in a position in the future to conduct terror activity against civil aviation targets.

Phoenix believes that the FBI should accumulate a listing of civil aviation universities/colleges around the country. FBI field offices with these types of schools in their area should establish appropriate liaison. FBIHQ should discuss this matter with other elements of the U.S. intelligence community and task the community for any information that supports Phoenix's suspicions. FBIHQ should consider seeking the necessary authority to obtain visa information from the USDOS on individuals obtaining visas to attend these types of schools and notify the appropriate FBI field office when these individuals are scheduled to arrive in their area of responsibility.

Phoenix has drawn the above conclusion from several Phoenix investigations to include captioned investigation and the following investigations: Arabian national and (b) (7), a Saudi (b) (7) and (b) (7).

as the result of investigation of [REDACTED] provided reliable information provided by [REDACTED] was initiated April 2000 that [REDACTED] information in the past. The source reported during the AL-MUHJIROUN. [REDACTED] was a supporter of UBL and [REDACTED]

Phoenix has identified several associates of [REDACTED] at [REDACTED] who arrived at the university around the same time that he did. These individuals are Sunni Muslims who have the same radical fundamentalists views as [REDACTED]. They come from [REDACTED]

To: Counterterrorism From: Phoenix
Re: [REDACTED] 07/10/2001

[REDACTED]
associates are:

[REDACTED] a [REDACTED]
[REDACTED] is enrolled in the [REDACTED]

[REDACTED] a [REDACTED]
enrolled in the [REDACTED] is

[REDACTED] an [REDACTED]
[REDACTED] is enrolled in the [REDACTED]

[REDACTED]
[REDACTED] is enrolled in the [REDACTED]

[REDACTED]
[REDACTED] is enrolled in the [REDACTED]

[REDACTED]
[REDACTED] enrolled in the [REDACTED] is

[REDACTED] The above individuals are involved with [REDACTED] and
regularly participate in meetings with him in [REDACTED] Arizona.

[REDACTED] FBIHQ, IRS [REDACTED] RFU, wrote an analytical
paper on the AL-MUHAJIROUN, dated 11/09/1999, in support of FBINY
investigation captioned: [REDACTED]

[REDACTED] can be found in [REDACTED] IRS [REDACTED] s research paper
was gleaned from IRS [REDACTED] s research paper. The following information

[REDACTED] The AL-MUHAJIROUN, which in English means THE
EMIGRANTS, is a Sunni Muslim fundamentalist organization based in the
United Kingdom. The organization's spiritual leader is SHEIKH OMAR
BAKRI MOHAMMED FOSTOK. The organization is dedicated to the overthrow

To: Counterterrorism From: Phoenix
Re: [REDACTED] 07/10/2001

[REDACTED] of Western society. British officials have reported that FOSTOK first came to their attention during the Gulf War after calling for the assassination of British Prime Minister John Major. FOSTOK has connections to UBL, JAMMAT AL-MUSLIMIAN (JM), HAMAS, HIZBALLAH and the ALGERIAN SALVATION FRONT.

[REDACTED] FOSTOK has made several controversial statements to the press. For example, he stated in public interviews that the bombings of the United States Embassies in Africa were "legitimate targets."

[REDACTED] FOSTOK, while representing the AL-MUHAJIROUN, signed a fatwa (religious decree) during February 1998 which stated the following:

[REDACTED] " The Fatwa is jihad against the U.S. and British government, armies, interests, airports (emphasis added by FBI Phoenix), and instructions and it has been given because of the U.S. and British aggression against Muslims and the Muslim land of Iraq...we...confirm that the only Islamic Fatwa against this explicit aggression is Jihad. Therefore the message for the British governments or any other government of non-Muslim countries is to stay away from Iraq, Palestine, Pakistan, Arabia, etc...or face full scale war of Jihad which it is the responsibility and the duty of every Muslim around the world to participate in...We...call upon...Muslims around the world including Muslims in the USA and in Britian to confront by all means whether verbally, financially, politically or militarily the U.S. and British aggression and do their Islamic duty in relieving the Iraqi people from the unjust sanctions."

[REDACTED] was interviewed by FBI Phoenix on [REDACTED]/2000 and [REDACTED]/2000. On [REDACTED]/2000, interviewing Agents observed photocopied photographs of UBL, IBN KHATTAB and wounded Chechnyan Mujahadin tacked to his livingroom wall. [REDACTED]

To: Counterterrorism From: Phoenix
Re: [REDACTED] 07/10/2001

Phoenix investigation of [REDACTED] ([REDACTED]) was predicated upon information received during

and [REDACTED] According to [REDACTED], a [REDACTED]

On 06/ [REDACTED] 2001, the [REDACTED] arrested two individuals who admitted under interrogation to being members of UBL's AL-QA'IDA organization. Evidence was developed demonstrating that these individuals were planning an operation to bomb the U.S. Embassy and U.S. Military forces in Saudi Arabia. A [REDACTED] passport [REDACTED] in the name of [REDACTED]

To: Counterterrorism From: Phoenix
Re: [REDACTED], 07/10/2001

[REDACTED]
[REDACTED] within their possession.

[REDACTED]'s [REDACTED] address and could be a relative.

Phoenix has not been able to show a direct association between [REDACTED] and [REDACTED] had departed the U.S. prior to [REDACTED]'s arrival. However, both [REDACTED] and [REDACTED] have associated with the [REDACTED] Arizona and it is highly probable that they know people in common.

Investigations of [REDACTED] and [REDACTED] were predicated on information received from [REDACTED] demonstrating that both subjects were involved with [REDACTED] activity. Both individuals also have association(s) with individuals associated with [REDACTED] who lived in Phoenix from the mid 1990s - 1997 left the United States after graduating from [REDACTED] has been identified as a friend of both [REDACTED] and [REDACTED].

[REDACTED] a known supporter of the [REDACTED]. Phoenix has not developed any information linking these [REDACTED] with the other subjects referenced in this communication.

Phoenix believes that it is more than a coincidence that subjects who are supporters of UBL are attending civil aviation universities/colleges in the State of Arizona. As receiving offices are aware, Phoenix has had significant UBL associates/operatives living in the State of Arizona and conducting activity in support of UBL. WADIH EL-HAGE, a UBL lieutenant recently convicted for his role in the 1998 bombings of U.S. Embassies in Africa, lived in Tucson, Arizona for several years during the 1980s. ESSAM AL-RIDI, a personal pilot for UBL, traveled to Tucson, Arizona during 1993 at the direction of AL-HAGE to procure a T-39 jet aircraft for UBL's personal use.

Phoenix believes that it is highly probable that UBL has an established support network in place in Arizona. This network was most likely established during the time period that EL-HAGE lived in Arizona.

To: Counterterrorism From: Phoenix
Re: [REDACTED], 07/10/2001

[REDACTED] This information is being provided to receiving
offices for information, analysis and comments.

[REDACTED]
To: Counterterrorism From: Phoenix
Re: [REDACTED] 07/10/2001

LEAD(s):

Set Lead 1:

COUNTERTERRORISM

AT WASHINGTON, DC

[REDACTED] The RFU/UBLU is requested to consider implementing the suggested actions put forth by Phoenix at the beginning of this communication.

Set Lead 2:

NEW YORK

AT NEW YORK, NEW YORK

[REDACTED] Read and Clear

♦♦

[REDACTED]

June 18, 2004

The Honorable Glenn A. Fine
Office of the Inspector General
United States Department of Justice
Room 4322
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

Dear Mr. Fine:

**Re: OIG DRAFT AUDIT REPORT - A REVIEW OF THE FBI'S
HANDLING OF INTELLIGENCE INFORMATION RELATED TO
THE SEPTEMBER 11 ATTACKS**

Reference is made to your memorandums, dated May 24, 2004 and June 10, 2004, requesting the FBI review the first five chapters and the recommendations of the subject draft audit report for factual accuracy and for whether anything in the recommendations is classified or too sensitive for public release. In addition the memorandums sought our comments as to whether or not the FBI believed the recommendations and conclusions were either inaccurate or unwarranted. This document is the FBI's formal response to the factual inaccuracies which is attached and the report's recommendations. The classification and sensitivity review was provided under separate cover. (U)

On behalf of the Director, I want to thank you and your staff for this report and for the countless hours of hard work that it required. As you know, the FBI values the Office of the Inspector General's input as a comprehensive independent assessment of our operations and as a means of identifying weaknesses that require corrective action to strengthen our operations. That is why the Director requested your office to conduct this review shortly after the 9/11 tragedy. Based upon our review, your findings and recommendations are consistent with the FBI's internal reviews and with those of other oversight entities. I am pleased to inform you that the FBI has made significant progress not only on the recommendations proffered in your report but on all the issues discovered by our own internal assessments. (U)

Before responding to the individual recommendations, the OIG and the American public need to be made aware of the progress made by the Federal Bureau of Investigation (FBI) since the horrific attacks of September 11, 2001. If we only responded to the recommendations in the report, readers would have an incomplete picture of the progress we have made and perhaps have a difficult time piecing together

[REDACTED]

[REDACTED]

the information under sixteen different recommendations. Director Mueller has implemented a comprehensive plan that fundamentally transforms the FBI to enhance our ability to predict and prevent future acts of terrorism. We have overhauled our counterterrorism operations, expanded our intelligence capabilities, modernized our business practices and technology, and improved coordination with our partners. (U)

Director Mueller replaced a priority system which allowed supervisors a great deal of flexibility with a set of 10 priorities that strictly govern the allocation of personnel and resources in every FBI program and field office. Counterterrorism is now the overriding priority, and every terrorism lead is addressed, even if it requires a diversion of resources from other priority areas. (U)

To implement these new priorities, we increased the number of Special Agents assigned to terrorism matters and hired additional intelligence analysts and translators. We also established a number of operational units and entities that provide new or improved capabilities to address the terrorist threat. These include the 24/7 Counterterrorism Watch (CT Watch) and the National Joint Terrorism Task Force (NJTTF) to manage and share threat information; the Terrorism Financing Operation Section (TFOS) to centralize efforts to stop terrorist financing; document/media exploitation squads to exploit material found both domestically and overseas for its intelligence value; deployable "Fly Teams" to lend counterterrorism expertise wherever it is needed; the Terrorist Screening Center (TSC) and Foreign Terrorist Tracking Task Force (FTTTF) to help identify terrorists and keep them out of the United States; the Terrorism Reports and Requirements Section to disseminate FBI terrorism-related intelligence to the Intelligence Community; and the Counterterrorism Analysis Section to "connect the dots" and assess the indicators of terrorist activity against the U.S. from a strategic perspective. (U)

We centralized management of our Counterterrorism Program at Headquarters to limit "stove-piping" of information, to ensure consistency of counterterrorism priorities and strategy across the organization, to integrate counterterrorism operations here and overseas, to improve coordination with other agencies and governments, and to make senior managers accountable for the overall development and success of our counterterrorism efforts. (U)

The FBI is building an enterprise-wide intelligence program that has substantially improved our ability to strategically direct our intelligence collection and to fuse, analyze, and disseminate our terrorism-related intelligence. After passage of the USA PATRIOT Act, related Attorney General Guidelines, and the ensuing opinion by the Foreign Intelligence Surveillance Court of Review removed the barrier to sharing information between intelligence and criminal investigations, we quickly implemented a plan to integrate all our capabilities to better prevent terrorist attacks. Director Mueller elevated intelligence to program-level status, putting in place a formal structure and concepts of operations to govern FBI-wide intelligence functions, and establishing Field Intelligence Groups (FIGs) in every field office. (U)

Understanding that we cannot defeat terrorism without strong partnerships, we have enhanced the level of coordination and information sharing with state and municipal law enforcement personnel. We expanded the number of Joint Terrorism Task Forces (JTTFs), increased technological connectivity with our partners, and implemented new ways of sharing information through vehicles such as the FBI Intelligence Bulletin, the Alert System, and the Terrorist Screening Center. To improve coordination with other federal agencies and members of the Intelligence Community, we joined with our federal partners to establish the Terrorist Threat Integration Center, exchanged personnel, instituted joint briefings, and started using secure networks to share information. We also improved our relationships with foreign governments by building on the overseas expansion begun under Director Louis Freeh; by offering investigative and forensic support and training, and by working together on task forces and joint operations. Finally, the FBI has expanded outreach to minority communities, and improved coordination with private businesses involved in critical infrastructure and finance. (U)

The FBI is making substantial progress in upgrading our information technology to streamline our business processes and to improve our ability to search for and analyze information, draw connections, and share it both inside the Bureau and out. We have deployed a secure high-speed network, put new or upgraded computers on desktops, and consolidated terrorist information in a searchable central database. We developed, and are preparing to launch, the Virtual Case File management system that will revolutionize how the FBI does business. (U)

Re-engineering efforts are making our bureaucracy more efficient and more responsive to operational needs. We revised our approach to strategic planning, and we refocused our recruiting and hiring to attract individuals with skills critical to our counterterrorism and intelligence missions. We have developed a more comprehensive training program and instituted new leadership initiatives to keep our workforce flexible. We are modernizing the storage and management of FBI records. We also built, and continue to improve, an extensive security program with centralized leadership, professional security personnel, more rigorous security measures, and improved security education and training. (U)

These improvements have produced tangible and measurable results. We significantly increased the number of human sources and the amount of surveillance coverage to support our counterterrorism efforts. We developed and refined a process for briefing daily threat information, and considerably increased the number of FBI intelligence reports produced and disseminated. Perhaps most important, since September 11, 2001, we have participated in disrupting dozens of terrorist operations by developing actionable intelligence and better coordinating our counterterrorism efforts. (U)

Prior to September 11, 2001, the Bureau had no centralized structure for the national management of its Counterterrorism Program, and terrorism cases were routinely managed out of individual field offices. An al-Qa'ida case, for example, might have been run out of the New York Field Office; a HAMAS case might have been managed by the Washington Field Office. This arrangement functioned for years, and produced a number of impressive prosecutions. Once counterterrorism became our overriding priority,

[REDACTED]

however, it became clear that this arrangement had a number of failings in that it 1) "stove-piped" investigative intelligence information among field offices; 2) diffused responsibility and accountability between counterterrorism officials at FBI Headquarters and the SACs who had primary responsibility for the individual terrorism investigations; 3) allowed field offices to assign varying priorities and resource levels to terrorist groups and threats; 4) impeded oversight by FBI leadership, and 5) complicated coordination with other federal agencies and entities involved in the war against terrorism. For all these reasons, it became apparent that the Counterterrorism Program needed centralized leadership. (U)

In December 2001, the Director reorganized and expanded the Counterterrorism Division (CTD) and created the position of Executive Assistant Director (EAD) for Counterterrorism and Counterintelligence. (The Assistant Director of CTD reports to the EAD.) We now have the centralized management to run a truly national program – to coordinate counterterrorism operations and intelligence production domestically and overseas; to conduct liaison with other agencies and governments; and to establish clear lines of accountability for the overall development and success of our Counterterrorism Program. With this management structure in place, we are driving the fundamental changes that are necessary to accomplish our counterterrorism mission. (U)

We divided the operations of the Counterterrorism Division into branches, sections, and units, each of which focuses on a different aspect of the current terrorism threat facing the U.S. These components are staffed with intelligence analysts and subject matter experts who work closely with investigators in the field and integrate intelligence across component lines. This integration allows for real-time responses to threat information and quick communication with decision-makers and investigators in the field. (U)

The Bureau is designed, and has always operated, as a law enforcement and an intelligence agency. It has the dual mission: 1) to investigate and arrest perpetrators of completed crimes (the law enforcement mission) and 2) to collect intelligence that will help prevent future crimes and assist policy makers in their decision making (the intelligence mission). History has shown that we are most effective in protecting the U.S. when we perform these two missions in tandem. (U)

The FBI recognized that investigations could produce intelligence benefits beyond arrest and prosecution. Starting with the Ku Klux Klan cases in the 1960's and the Mafia cases of the 1970's, our agents began to view criminal investigations not only as a means of arresting and prosecuting someone for a completed crime, but also as a means of obtaining information to prevent future crime. The goal was not simply to arrest individual members of the Klan or the Mafia, but to penetrate and dismantle the whole criminal organization. (U)

As this approach was adopted, the FBI further developed the intelligence tools – such as electronic surveillance and the cultivation of human sources – that are critical to predicting and preventing criminal activity. We also learned to think strategically before

[REDACTED]

making arrests, sometimes opting to delay a suspect's arrest to allow more opportunity for surveillance that might disclose other conspirators or other criminal plans. We have used this approach to great effect in organized crime cases and espionage investigations, and members of our Safe Streets Task Forces use it in their fight against street gangs. (U)

This is the approach that is needed to prevent terrorism. Prior to September 11th, however, we were handicapped in our ability to implement this approach in the counterterrorism arena for two primary reasons. (U)

First, judicial rules and DOJ internal procedures prohibited our counterterrorism agents working intelligence cases from coordinating and sharing information with criminal agents who often were working investigations against the same targets. Second, we had not developed the institutional structure and processes necessary for a fully functioning intelligence operation. We started to address each of these problems immediately after the September 11, 2001 attacks. (U)

By definition, investigations of international terrorism are both "intelligence" and "criminal" investigations. They are intelligence investigations because their objective, pursuant to Executive Order 12333, is "the detection and countering of international terrorist activities," and because they employ the authorities and investigative tools – such as Foreign Intelligence Surveillance Act warrants – that are designed for the intelligence mission of protecting the U.S. against attack or other harm by foreign entities. They are criminal investigations since international terrorism against the U.S. constitutes a violation of the federal criminal code. (U)

Over the past two decades, a regime of court rules and internal DOJ procedures developed surrounding the use of FISA warrants that barred FBI agents and other Intelligence Community personnel working intelligence cases that employed the FISA tool from coordinating and swapping leads with agents working criminal cases. As a result of this legal "wall," "intelligence" agents and "criminal" agents working on a terrorist target had to proceed without knowing what the other may have been doing about that same target. In short, we were fighting international terrorism with one arm tied behind our back. (U)

The USA PATRIOT Act, enacted on October 26, 2001 eliminated this "wall" and authorized coordination among agents working criminal matters and those working intelligence investigations. On March 6, 2002 the Attorney General issued new Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI (Intelligence Sharing Procedures) to capitalize on this legislative change. The new procedures specifically authorized agents working intelligence cases to disseminate to criminal prosecutors and investigators all relevant foreign intelligence information, including information obtained from FISA, in accordance with applicable minimization standards and other specific restrictions (originator controls). Likewise, the procedures authorized prosecutors and criminal agents to advise FBI agents working intelligence cases on all aspects of foreign intelligence investigations, including the use of FISA. (U)

[REDACTED]

[REDACTED]

On November 18, 2002 the Foreign Intelligence Surveillance Court of Review issued an opinion approving the Intelligence Sharing Procedures, thereby authorizing the FBI to share information, including FISA-derived information, between our criminal and intelligence investigations. With this opinion, we were finally able to conduct our terrorism investigations with the full use and coordination of our criminal and intelligence tools and personnel. (U)

To formalize this merger of intelligence and criminal operations, we have abandoned the separate case classifications for "criminal" international terrorism investigations (with the classification number 265) and "intelligence" international terrorism investigations (classification number 199), and have consolidated them into a single classification for "international terrorism" (new classification number 315). This reclassification officially designates an international terrorism investigation as one that can employ intelligence tools as well as criminal processes and procedures. In July 2003, we formalized this approach in our Model Counterterrorism Investigative Strategy (MCIS), which was issued to all field offices and has been the subject of extensive field training. (U)

With the dismantling of the legal "wall" and the integration of our criminal and intelligence personnel and operations, we now have the latitude to coordinate our intelligence and criminal investigations and to use the full range of investigative tools against a suspected terrorist. On the intelligence side, we can conduct surveillance on the suspected terrorist to learn about his movements and identify possible confederates; we can obtain FISA authority to monitor his conversations; and/or we can approach and attempt to cultivate him as a source or an operational asset. On the criminal side, we have the option of incapacitating him through arrest, detention, and prosecution. We decide among these options by continuously balancing the opportunity to develop intelligence against the need to apprehend the suspect and prevent him from carrying out his terrorist plans. This integrated approach has guided our operations and we have successfully foiled terrorist-related operations and disrupted cells from Seattle, Washington, to Detroit, Michigan, to Lackawanna, New York. (U)

Although we are now able to coordinate our intelligence collection and criminal law enforcement operations, we can only realize our full potential as a terrorism prevention agency by developing the intelligence structure, capabilities, and processes to direct those operations. Without an effective intelligence capacity, we cannot expect to defeat a sophisticated and opportunistic adversary like al-Qa'ida. (U)

For a variety of historical reasons, the Bureau had not developed this intelligence capacity prior to September 11. While the FBI has always been one of the world's best collector of information, we never established the infrastructure to exploit that information fully for its intelligence value. Individual FBI agents have always analyzed the evidence in their particular cases, and then used that analysis to guide their investigations. The FBI as an institution, however, had not elevated that analytical process above the individual case or investigation to an overall effort to analyze

[REDACTED]

intelligence and strategically direct intelligence collection against threats across all programs. (U)

The attacks of September 11, 2001 highlighted the need to develop an intelligence process for the Counterterrorism Program and the rest of the Bureau. Since then, we have undertaken to build the capacity to fuse, analyze, and disseminate our terrorism-related intelligence, and to direct investigative activities based on our analysis of gaps in our collection against national intelligence requirements. That effort has proceeded in four stages. (U)

Our first step was to increase the number of analysts working on counterterrorism. Immediately after September 11, we temporarily reassigned analysts from the Criminal Investigative Division and Counterintelligence Division to various units in the Counterterrorism Division. In July 2002, 25 analysts were detailed from the CIA to assist our counterterrorism efforts. Many of these analysts provided tactical intelligence analysis; others provided strategic "big picture" analysis. All of them worked exceptionally hard and helped us analyze the mass of data generated in the aftermath of the terrorist attacks. These deployments were a temporary measure, but the progress made, the confidence gained, and the lessons learned during this period started us down the road toward a functioning intelligence analysis operation. We also established the College of Analytical Studies to help train and develop our own cadre of analysts. (U)

On December 3, 2001, the Director established the Office of Intelligence (OI) within the Counterterrorism Division. The OI was responsible for establishing and executing standards for recruiting, hiring, training, and developing the intelligence analytic workforce, and ensuring that analysts are assigned to operational and field divisions based on intelligence priorities. Recognizing that intelligence and analysis are integral to all of the Bureau's programs, in February 2003, Director Mueller moved the OI out of the Counterterrorism Division and created a stand-alone OI, headed by an Executive Assistant Director (EAD-I), to provide centralized support and guidance for the Bureau's intelligence functions. (U)

The next step in our intelligence integration was to elevate intelligence functions to program-level status, instituting centralized management and implementing a detailed blueprint for the Intelligence Program. (U)

The Director articulated a clear mission for the Intelligence Program – to position the FBI to meet current and emerging national security and criminal threats by: 1) aiming investigative work proactively against threats; 2) building and sustaining enterprise-wide intelligence policies and capabilities; and 3) providing useful, appropriate, and timely information and analysis to the national security, homeland security, and law enforcement communities. We then set out to embed intelligence processes into the day-to-day work of the FBI, from the initiation of a preliminary investigation to the development of FBI-wide strategies. (U)

[REDACTED]

Now that the Intelligence Program is established and developing, the FBI is moving on to the next stage of transforming the Bureau into an intelligence agency – reformulating personnel and administrative procedures to instill within our workforce an expertise in the processes and objectives of intelligence work. (U)

A major element of the Bureau's transformation is our increasing integration and coordination with our partners in the U.S. and international law enforcement and intelligence communities. More than any other type of enforcement mission, counterterrorism requires the participation of every level of local, state, national, and international government. A good example is the case of the Lackawanna terrorist cell outside Buffalo, New York. From the police officers who helped to identify and conduct surveillance on the cell members; to the CIA officers who provided information from their sources overseas; to the diplomatic personnel who coordinated our efforts with foreign governments; to the FBI agents and federal prosecutors who conducted the investigation leading to the arrests and indictment, everyone played a significant role. (U)

We recognize that a prerequisite for any operational coordination is the full and free exchange of information. Without procedures and mechanisms that allow information sharing on a regular and timely basis, we and our partners cannot expect to align our operational efforts to best accomplish our shared mission. Accordingly, we have taken steps to establish unified FBI-wide policies for sharing information and intelligence. (U)

To ensure a coordinated, enterprise-wide approach, the Director recently designated the EAD-I to serve as the principal FBI official for information and intelligence sharing policy. In this capacity, the EAD-I functions as an advisor to the Director and provides policy direction on information and intelligence sharing within and outside the FBI with the law enforcement and intelligence communities, as well as foreign governments. (U)

On February 20, 2004 we formed an information sharing policy group, comprised of Executive Assistant Directors, Assistant Directors and other senior executive managers. Under the Direction of the EAD-I, this group is establishing FBI information and intelligence sharing policies. (U)

On February 11, 2004 the Attorney General announced the creation of the DOJ Intelligence Coordinating Council. The Council is comprised of the heads of DOJ agencies with intelligence responsibilities, and is currently chaired by the FBI's EAD-I. The Council will work to improve information sharing within DOJ and to ensure that DOJ meets the intelligence needs of outside customers and acts in accordance with intelligence priorities. It will also identify common challenges (such as electronic connectivity, collaborative analytic tools, and intelligence skills training) and establish policies and programs to address them. (U)

Beyond these information sharing initiatives, we are increasing our operational coordination with our state, federal, and international partners on a number of fronts. (U)

[REDACTED]

We have established much stronger working relationships with the CIA and other members of the Intelligence Community. From the Director's daily meetings with the Director of Central Intelligence and CIA briefers, to our regular exchange of personnel among agencies, to our joint efforts in specific investigations and in the Terrorist Threat Integration Center, the Terrorist Screening Center, and other multiagency entities, the FBI and its partners in the Intelligence Community are now integrated at virtually every level of our operations. (U)

The Terrorist Threat Integration Center is a good example of our collaborative relationship with the CIA and other federal partners. Established on May 1, 2003 at the direction of President Bush, TTIC coordinates strategic analysis of threats based on intelligence from the FBI, CIA, DHS, and DOD. Analysts from each agency work side-by-side in one location to piece together the big picture of threats to the U.S. and our interests. TTIC analysts synthesize government-wide information regarding current terrorist threats and produce the Presidential Terrorism Threat Report for the President. The FBI personnel at TTIC are part of the Office of Intelligence and work closely with analysts at FBI Headquarters in combining domestic and international terrorism developments into a comprehensive analysis of terrorist threats. In addition to the analysis developed by FBI analysts detailed to TTIC, FBI analysts at Headquarters regularly contribute articles to the President's Terrorist Threat Report. (U)

The FBI currently has Agents and Analysts detailed to CIA entities, including the CIA's Counter Terrorism Center (CTC). We also have FBI agents and intelligence analysts detailed to the NSA, the National Security Council, DIA, the Defense Logistics Agency, DOD's Regional Commands, the Department of Energy, and other federal and state agencies. (U)

CIA personnel are also working in key positions throughout the Bureau. The Associate Deputy Assistant Director for Operations in the Counterterrorism Division is a CIA detailee. CIA officers are detailed to the Security Division, including the Assistant Director, the Chief of the Personnel Security Section, and managers working with the Secret Compartmental Information (SCI) program and the FBI Police. An experienced manager from the CIA's Directorate of Science and Technology now heads the Investigative Technologies Division and a Section Chief in that division is on rotation from CIA. (U)

This exchange of personnel is taking place in our field offices as well. In 33 field locations, the CIA has officers co-located with FBI agents at JTTF sites, and there are plans to add CIA officers to several additional sites. The NSA has analysts detailed to FBI Headquarters, the Washington Field Office, the New York Field Office, and the Baltimore Field Office. (U)

Each morning, in addition to FBI Briefs, the Director is briefed by a CIA briefer. The Director of Central Intelligence and the FBI Director then jointly brief the President

[REDACTED]

on current terrorism threats. In addition, CIA and DHS personnel attend the Director's internal terrorism briefings every weekday morning and afternoon. (U)

The FBI is now using secure systems to disseminate classified intelligence reports and analytical products to the Intelligence Community and other federal agencies. The FBI hosts a web site on the Top-Secret Intelink/Joint World-Wide Intelligence Community System (JWICS), a fully-encrypted system that connects more than 100 Department of Defense, CIA, and other Intelligence Community sites. We also host a web site on SIPRNET, a similar system used by DOD for sharing information classified at the Secret level. In addition, a new TS/SCI network known as "SCION" is being piloted in several field offices. SCION will connect FBI Headquarters and field offices to the CIA and other members of the Intelligence Community, and will increase opportunities for inter-agency collaboration. (U)

Improving the compatibility of information technology systems throughout the Intelligence Community will increase the speed and ease of information sharing and collaboration. Accordingly, the FBI's information technology team has worked closely with the Chief Information Officers (CIOs) of DHS and other Intelligence Community agencies, to develop our recent and ongoing technology upgrades. This coordination has affected our decisions on several key technology upgrades. (U)

To facilitate further coordination, the FBI CIO sits on the Intelligence Community CIO Executive Council. The Council develops and recommends technical requirements, policies and procedures, and coordinates initiatives to improve the interoperability of information technology systems within the Intelligence Community. It was established by Director of Central Intelligence directive and is chaired by the CIA's CIO. (U)

DHS plays a critical role in assessing and protecting vulnerabilities in our national infrastructure and at our borders, and in overseeing our response capabilities. We have worked closely with DHS to ensure that we have the integration and comprehensive information sharing between our agencies that are vital to the success of our missions. The FBI and DHS share database access at TTIC, in the National JTTF at FBI Headquarters, in the FTTTF and the TSC, and in local JTTFs in our field offices around the country. We worked closely together to get the new Terrorist Screening Center up and running. We hold weekly briefings in which our CTD analysts brief their DHS counterparts on current terrorism developments. We coordinate all FBI warnings with DHS, and we now coordinate joint warnings through the Homeland Security Advisory System to address our customers' concerns about multiple and duplicative warnings. We designated an experienced executive from the Transportation Security Administration to run the TSC and detailed a senior DHS executive to the FBI's Office of Intelligence to ensure coordination and transparency between the agencies. (U)

On March 4, 2003, the Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence signed a comprehensive Memorandum of Understanding (MOU) establishing policies and procedures for information sharing, handling, and use. Pursuant to that MOU, information related to terrorist threats and

[REDACTED]

[REDACTED]

vulnerabilities is provided to DHS automatically without DHS having to request it. Consistent with the protection of sensitive sources and methods and the protection of privacy rights, we now share as a rule, and withhold by exception. (U)

With terrorists traveling, communicating, and planning attacks all around the world, coordination with our foreign partners has become more critical than ever before. We have steadily increased our overseas presence and now routinely deploy agents and crime scene experts to assist in the investigation of overseas attacks, such as the May 2003 bombings in Saudi Arabia and Morocco. As of January 7, 2004, 413 FBI personnel were assigned overseas, over 200 of whom are permanently assigned. Their efforts, and the relationships that grow from them, have played a critical role in the successful international operations we have conducted over the past 31 months. (U)

Bureau personnel have participated in numerous investigations of terrorist attacks in foreign countries over the past 33 months. Our approach to those investigations differs from the approach we traditionally have taken. Prior to September 11th, our overseas investigations primarily were focused on building cases for prosecution in the U.S. Today, our focus has broadened to provide our foreign partners with investigative, forensic, and other types of support which enhance our joint efforts to prevent and disrupt terrorist attacks. Our partners have embraced this approach, and it is paying dividends with greater reciprocal cooperation and more effective joint investigations. (U)

The foundation of a centralized and effective counterterrorism operation is the capability to assemble, assimilate, and disseminate investigative and operational information both internally and with fellow intelligence and law enforcement agencies. This capability requires information technology (IT) that makes information easily accessible and usable by all personnel while protecting the security of that information. (U)

Prior to September 11th, the Bureau's information technology was inadequate to support its counterterrorism mission. In previous years, substantial investments were made to upgrade technologies that directly supported investigations, such as surveillance equipment and forensic services like the Integrated Automated Fingerprint Identification System. Insufficient attention was paid, however, to technology related to the more fundamental tasks of records creation, maintenance, dissemination, and retrieval. In 2001, many employees still used vintage 1987 386 desktop computers. Some resident agencies could only access data in their field office via a slow dial-up connection. Many Bureau programs were using computer systems that operated independently and did not interoperate with systems in other programs or other parts of the Bureau. (U)

The FBI also had a deficient information management system. The FBI's legacy investigative information system, the Automated Case Support (ACS), was not very effective in identifying information or supporting investigations. Users navigated with the function keys instead of the "point and click" method common to web-based applications. Simple tasks, such as storing an electronic version of a document, required a user to perform 12 separate functions in a "green screen" environment. Also, the system lacked

[REDACTED]

multimedia functionality to allow for the storage of information in its original form. Agents could not store many forms of digital evidence in an electronic format, instead having to describe the evidence and indicate where the evidence was stored in a control room. (U)

Thanks to the character and resolve of its personnel, the FBI was able to achieve numerous investigative successes, in spite of these obstacles. It was clear as of September 11, however, that we needed an integrated IT infrastructure to manage our information. We brought on-board a highly skilled team of experts and set out to create an IT infrastructure that is fast and secure, and that ties together the applications and databases used throughout the Bureau. We also designed user-friendly, web-based software applications to reduce reliance on paper records and to streamline investigative workflow. These improvements are enhancing our ability to collect, store, search, analyze, and share information. (U)

The first step in the FBI's modernization effort is the Trilogy Program, a multi-year effort to enhance our effectiveness through technologies that allow us to better access, organize, and analyze information. The Trilogy Program is aimed at providing all FBI offices, including overseas Legal Attaché offices, with improved network communications, a common and current set of office automation tools, and user-friendly web-based applications. Trilogy upgrades also incorporate controls to provide an enhanced level of security for FBI information. (U)

Following September 11, we saw the need to provide counterterrorism investigators and analysts with quick, easy access to the full breadth of information relating to terrorism. We developed a three-step plan that would provide immediate support to counterterrorism and then incrementally increase the range and effectiveness of that support for other criminal investigations. This plan transitions us away from separate systems containing separate data, towards an Investigative Database Warehouse (IDW) that contains all data that can legally be stored together. The IDW provides the Bureau with a single access point to several data sources that were previously available only through separate, stove-piped systems. By providing consolidated access to the data, for the first time analytical tools can be used across data sources to provide a more complete view of the information possessed by the Bureau. (U)

The initial step toward the IDW was the implementation of the Secure Counterterrorist Operational Prototype Environment (SCOPE) program. Under the SCOPE program we quickly consolidated counterterrorism information from various data sources, providing analysts at Headquarters with substantially greater access to more information in far less time than with other FBI investigative systems. The SCOPE database also gave us an opportunity to test new capabilities in a controlled environment. This prototype environment has now been replaced by the IDW. (U)

The IDW, delivered in its first phase to the Office of Intelligence in January 2004, now provides analysts with full access to investigative information within FBI files, including ACS and VGTOF data, open source news feeds, and the files of other federal

[REDACTED]

agencies such as DHS. The IDW provides physical storage for data and allows users to access that data without needing to know its physical location or format. The data in the IDW is at the Secret level, and the addition of TS/SCI level data is in the planning stages. (U)

Later this year, we plan to enhance the IDW by adding additional data sources, such as Suspicious Activity Reports, and by making it easier to search. When the IDW is complete, agents and analysts using new analytical tools will be able to search rapidly for pictures of known terrorists and match or compare the pictures with other individuals in minutes rather than days. They will be able to extract subjects' addresses, phone numbers, and other data in seconds, rather than searching for it manually. They will have the ability to identify relationships across cases. They will be able to search up to 100 million pages of international terrorism-related documents in seconds. (U)

Ultimately, we plan to turn the IDW into a Master Data Warehouse (MDW) that will include the administrative data required by the FBI to manage its internal business processes in addition to the investigative data. MDW will grow to eventually provide physical data storage for, and become the system of record for, all FBI electronic files. (U)

We are introducing advanced analytical tools to help us make the most of the data stored in the IDW. These tools allow FBI agents and analysts to look across multiple cases and multiple data sources to identify relationships and other pieces of information that were not readily available using older FBI systems. These tools 1) make database searches simple and effective; 2) give analysts new visualization, geo-mapping, link-chart capabilities and reporting capabilities; and 3) allow analysts to request automatic updates to their query results whenever new, relevant data is downloaded into the database. (U)

As the first part of our IT modernization efforts near completion, FBI agents, analysts, and support personnel are already enjoying new capabilities and applying those capabilities to their counterterrorism mission. They have up-to-date desktops, fast and secure connectivity, a user-friendly interface to the ACS case management system, the ability to access and search consolidated terrorism-related data, and new capabilities for sharing information inside and outside the Bureau. (U)

While there is still much to be done, these efforts are starting to deliver the technology we need to stay ahead of evolving threats. Upgrading our technology will remain an FBI priority for the foreseeable future, and our new IT management will ensure that we continue to improve our systems. (U)

With the recent directives implementing the intelligence agent career track and the administrative reforms related to building an intelligence workforce, we have in place the essential structural elements of an intelligence-driven counterterrorism operation. The challenge now is to refine and continue to develop that operation – an effort that will require additional resources, continued attention by FBI leadership, and constant training of FBI personnel in intelligence processes and objectives. (U)

[REDACTED]

While we have clearly made substantial progress over the past 33 months, it is difficult to come up with an exact measurement of the current effectiveness of our counterterrorism efforts. Besides citing the absence of successful attacks on the homeland since September 11th, there is no single measure that completely captures the progress we have made. There are several yardsticks, however, that demonstrate the effectiveness of the core functions of a Counterterrorism Program. These yardsticks include the following:

- Development of human assets
- Number of FISAs
- Number of intelligence reports generated
- Quality of daily briefings
- Effectiveness of counterterrorism operations
- Continued protection of civil liberties

An application of these yardsticks demonstrates the progress we have achieved since September 11, 2001. (U)

The FBI has long recognized that human source information is one of the most important ways to investigate criminal activity. We have long-standing expertise in recruiting and using human sources, and we have used those skills to great effect across a wide range of investigative programs, including organized crime, drugs, public corruption, and white collar crime. (U)

While we also have developed sources over the years in the Counterterrorism Program, September 11th highlighted the shortage of human intelligence reporting about al-Qa'ida both in the U.S. and abroad. With the U.S. government having relatively few assets who were able to penetrate and report on al-Qa'ida's plans, we were vulnerable to surprise attack. (U)

The Bureau has placed a priority on developing human intelligence sources reporting on international terrorists. We have revised our training program, our personnel evaluation criteria, and our operational priorities to focus on source development. While we continue to grow this capacity, we have already seen a marked increase in the number of human intelligence sources in the Counterterrorism Program. Between August 30, 2001, and September 30, 2003, the number of sources related to international terrorism increased by more than 60 percent, and the number of sources related to domestic terrorism increased by more than 39 percent. (U)

FISA coverage has also increased significantly, reflecting both our increased focus on counterterrorism and counterintelligence investigations and improvement in the operation of the FISA process. From 2001 to 2003, the number of FISA applications filed annually with the Foreign Intelligence Surveillance Court increased by 85 percent. We have seen a similar increase in the use of the emergency FISA process that permits us to obtain immediate coverage in emergency situations. In 2002, for example, the Department of Justice obtained a total of 170 emergency FISA authorizations, which is more than three times the number of emergency FISAs we obtained in the 23 years between the 1978 enactment of FISA and September 11, 2001. (U)

[REDACTED]

[REDACTED]

In the past year, the FBI produced more than 3,000 intelligence products, including "raw" reports, intelligence memoranda, in-depth strategic analysis assessments, special event threat assessments, and focused Presidential briefings. We also conducted numerous intelligence briefings to members of Congress, other government agencies, and the law enforcement and intelligence communities. These efforts mark a new beginning for the FBI's intelligence operation. (U)

Prior to September 11, 2001, the FBI produced very few raw intelligence reports. In FY 2003, we produced and disseminated 2,425 Intelligence Information Reports (IIRs) containing raw intelligence derived from FBI investigations and intelligence collection. The majority contained intelligence related to international terrorism; the next greatest number contained foreign intelligence and counterintelligence information; and the remainder concerned criminal activities and cyber crime. These IIRs were disseminated to a wide customer set in FBI field offices, the Intelligence Community, Defense Community, other federal law enforcement agencies, and U.S. policy entities. (U)

In addition to these raw intelligence reports, the FBI has begun producing analytic assessments on a par with those of the Intelligence Community. The FBI developed and issued, in January 2003, a classified comprehensive assessment of the terrorist threat to the U.S. This assessment focuses on the threats that the FBI sees developing over the next two years, based on an analysis of information regarding the motivations, objectives, methods, and capabilities of existing terrorist groups and the potential for the emergence of new terrorist groups and threats throughout the world. This threat assessment is used as a guide in the allocation of investigative resources, as a useful compilation of threat information for investigators and intelligence personnel within and without the FBI, and as a resource for decision-makers elsewhere in the government. The 2004 threat assessment was released in April 2004. FBI analysts have produced over 100 in-depth analyses and several hundred current intelligence articles in addition to the work they do assisting FBI investigations. (U)

We are preparing to produce, in the near future, the *FBI Daily Report* and the *FBI National Report* to provide daily intelligence briefings to personnel in the field and external customers. One will be produced at the classified level and limited in distribution to upper-level field managers. The other will be unclassified and widely distributed to field office personnel and our partners in the law enforcement community. (U)

A good example of our ability to exploit evidence for its intelligence value and share that intelligence is our use of the al-Qa'ida terrorism handbook. A terrorism handbook seized from an al-Qa'ida location overseas in the mid-1990's was declassified and released by DOJ shortly after the events of September 11, 2001. We determined that intelligence gleaned from the handbook could provide useful guidance about al-Qa'ida's interests and capabilities. Accordingly, we produced and disseminated a series of intelligence products to share this intelligence with our personnel in the field and with our law enforcement partners. Nine Intelligence Bulletins were based in whole or in part on this intelligence. In addition, we used information derived from the al-Qa'ida Handbook

[REDACTED]

to update our counterterrorism training, including the Intelligence Analyst Basic Course at the College of Analytical Studies, the Introduction to Counterterrorism Course at the National Academy, and sessions on Terrorism Indicators and Officer Safety in our SLATT training. The unclassified version of the handbook is now maintained as a reference in the FBI Library and is accessible to all the students at the Academy. It also is included in the reference manual CD-Rom distributed as part of SLATT training. (U)

One telling measure of our improved counterterrorism operations is the development of our capability to brief the daily terrorist threat information. The development of this capability reflects the maturing of our centralized Counterterrorism Program. (U)

Prior to September 11th, the FBI lacked the capacity to provide a comprehensive daily terrorism briefing – to assemble the current threat information, to determine what steps were being taken to address each threat, and to present a clear picture of each threat and the Bureau's response to that threat to the Director, senior managers, the Attorney General, and others in the Administration who make operational and policy decisions. With a decentralized program in which investigations were run by individual field offices, the Bureau never had to develop this specialized skill. With the need for centralized management, however, it became an imperative. (U)

In the aftermath of the terrorist attacks, we were asked to begin sending to the White House each morning daily reports on counterterrorism-related events. We had no mechanism in place for collecting that information, so preparation of the reports was initially haphazard. During the past 33 months, with the assistance of veterans from the Intelligence Community, we have established the infrastructure and the cadre of professionals to produce effective daily briefings and to share briefing materials more widely within the Bureau and with our partners. (U)

In 2002 we established the Presidential Support Group within the Counterterrorism Division to prepare daily briefing materials. In the summer of 2003, this group was renamed the Strategic Analysis Unit and moved to the Office of Intelligence. Beginning in August 2003, the Strategic Analysis Unit began producing the Director's Daily Report (DDR), a daily intelligence briefing that includes information on counterterrorism operations, terrorism threats, and information related to all areas of FBI investigative activity. (U)

To produce the DDR, the Strategic Analysis Unit consolidates and refines information provided in a standardized format by intelligence personnel in each division. Each morning, information about new threats is added, and information about threats that have been thoroughly vetted during the night is removed. The DDR is distributed to executives in all FBI operational divisions. The Director uses the DDR to brief the President nearly every weekday morning. The FBI also produces the *Presidential Intelligence Assessment*, a finished FBI intelligence product covering topics of particular interest to the President, and as noted earlier, our personnel at TTIC and at FBI

[REDACTED]

Headquarters contribute to the formulation of the daily *President's Terrorist Threat Report*. (U)

Director Mueller holds threat briefings twice a day: an intelligence briefing in the morning and a case-oriented briefing in the evening. At these briefings, a briefer and the operational executive managers provide a summary of the current threats and our operations. With CIA and DHS representatives in attendance, these meetings also serve to ensure that all threat information is appropriately passed to those agencies. (U)

The development of this daily briefing operation is a tangible measure of the progress we have made since the day when terrorism investigations were run by individual field offices and little effort was made to centrally direct or coordinate them throughout the Bureau and with the other agencies involved in protecting the U.S. against terrorism. (U)

The Bureau historically measured its performance, to a large extent, by the number of criminals it arrested. While useful for traditional law enforcement, where the primary objective is arrest and prosecution, this standard is under-inclusive as applied to counterterrorism, where the primary objective is to neutralize terrorist threats. It only captures that subset of terrorist threats that are neutralized by arresting terrorists and prosecuting them with charges of criminal terrorism. It fails to capture the terrorist threats we neutralize through means other than formal terrorism prosecutions – such as deportation, detention, arrest on non-terrorism charges, seizure of financial assets, and the sharing of information with foreign governments for their use in taking action against terrorists within their borders. (U)

A more useful measure is one we have used in organized crime cases – the number of disruptions and dismantlements. This measure counts every time we – either by ourselves or with our partners in the law enforcement and intelligence communities – conduct an operation which disables, prevents, or interrupts terrorist fundraising, recruiting, training, or operational planning. Since September 11, 2001, the FBI has participated in dozens of such operations, disrupting a wide variety of domestic and international terrorist undertakings. (U)

While the number of disruptions is significant, the most telling measure of our progress is the manner in which we have conducted individual operations consistent with our prevention mission. The extent of our transformation is most clearly seen in the approach we take when confronting specific terrorist threats. Our approach to these operations demonstrates the extent to which coordination and prevention through the development of actionable intelligence have become our guiding operational principles. (U)

The September 11, 2001, terrorist attacks awakened all of us to the deadly threat of modern terrorism and to the need for bold action. We in the FBI have undertaken that bold action over the past 33 months. While there is still much work to be done, we have made significant progress. With these efforts, and with the unwavering support of the American people, we are confident that we will prevail in our war against terrorism. (U)

[REDACTED]

SPECIFIC RESPONSES TO OIG RECOMMENDATIONS:

A. Recommendations related to the FBI's analytical program: (U)

Recommendation No. 1: Improve the hiring, training and retention of intelligence analysts. (U)

Response: The FBI has taken a number of measurable steps to improve the hiring, training, and retention of analysts since the September 11 attacks. (U)

- The FBI's Office of Intelligence (OI), led by an Executive Assistant Director who is a career intelligence analyst in the U.S. Intelligence Community, has developed a recruiting plan to ensure that the FBI actively recruits candidates with the critical skills necessary to provide world-class intelligence analysis for the FBI's mission. In September 2003, the Director approved the FBI's Human Talent for Intelligence Production Concept of Operations (CONOPS), which focuses on the recruitment, hiring, development, and training of intelligence analysts. (U)
- **Recruitment/Hiring:** Prior to the approval of the Human Talent CONOPS the FBI did not have a recruitment effort specific to the intelligence analyst position. As such, intelligence analysts were not routinely part of recruitment teams. In an effort to ensure the FBI is prepared to meet emerging recruitment and hiring priorities for intelligence analysts, the OI selected intelligence analysts (FBIHQ and field) to serve as intelligence analyst recruiters. The intelligence analyst recruiters attend events at colleges and universities, as well as designated conferences and career fairs throughout the country. From October 2003 - April 2004, the FBI participated in more than 10 recruitment events and plans to participate in at least five additional events through September 2004. (U)
- A marketing plan was also implemented to supplement the Intelligence Analyst recruiting efforts. On February 8, 2004, an advertisement specific to the intelligence analyst position at the FBI was placed in the Washington Post, Washington Times, and the New York Times, and has since been re-advertised several times. On February 9, 2004, the first press release addressing intelligence analyst recruitment at the FBI was released by the FBI National Press Office kicking off an aggressive intelligence analyst hiring campaign. And, on February 17, 2004, the second press release was released featuring an interview with EAD for Intelligence Maureen A. Baginski and two FBI Intelligence Analysts. (U)
- In 2004, the FBI revised its hiring procedures for Intelligence Analysts to more effectively recruit and hire candidates with necessary critical skills. The new system is a resume and weighted question-based system. The weighted questions were developed by a group of senior intelligence analysts and intelligence analyst managers under the direction of the EAD for Intelligence, and were designed to identify the most highly-qualified candidates at all entry grade levels. Aside from direct recruitment into the intelligence analyst position, the OI is establishing

education cooperative programs wherein college students would have an arrangement to work at the FBI and earn a four-year degree. Students may alternate semesters of work with full-time study or may work in the summers in exchange for tuition assistance. The program targets students who intend to complete a four-year degree in disciplines needed for FBI Intelligence Analyst work to include: International Studies; Foreign Languages; Studies pertinent to specific geographic areas and cultures; History; Economics; Business; Political Science; Public Administration; Physical Sciences; and Journalism. In addition to financial assistance, students would benefit by obtaining significant work experience, and the FBI would benefit through an agreement by the student to continue working for the FBI for a period of time upon completion of their education. (U)

- College of Analytic Studies: Since Fiscal Year 2002, the College of Analytic Studies (CAS) has delivered 13 iterations of the Basic Intelligence Analysis Course for newly hired analysts. In addition, through intelligence community partnerships and private vendors, the CAS has coordinated specialized training for novice and experienced FBI Intelligence Analysts. (U)
 - 264 FBI Analysts have graduated from the College's six-week Basic Intelligence Analyst Course since its establishment. (U)
 - 655 FBI field and headquarters Analysts have attended specialty courses on a variety of topics such as analytical methods, tools, and databases. (U)
- 1,389 FBI field and headquarters personnel (Analysts and Agents) have attended specialized counterterrorism courses offered in conjunction with CIA University. (U)
- ACES I: The Basic Intelligence Analyst Course currently offered by the CAS is being revised/updated. Upon completion of this effort the course will be re-titled: Analytical Cadre Education Strategy I (ACES I) as outlined in the Human Talent Conops. The ACES I course will incorporate seven core elements for intelligence training for new agents and new analysts. Additionally the new course curriculum teaches advanced analytic trade craft and practice, thinking and writing skills, resources, and field skills. An intermediate course entitled ACES II is anticipated in the future that would target more experienced analysts. (U)
 - Mentoring Program: The OI is creating a career mentoring program to provide guidance and advice to Intelligence Analysts on the analytical career in the FBI. Once implemented, all new Intelligence Analysts (new to the position or new to the FBI) will have a mentor to assist them. This program will be implemented in calendar year 2004. (U)

Recommendation No. 2: Ensure effective management of analysts. (U)

[REDACTED]

Response: The FBI agrees that it must do all that it can to ensure that its dedicated Intelligence Analysts receive effective management support and direction. Since September 11, 2001, a number of changes have taken place to improve the management of Intelligence Analysts. The EAD-I and the OI have immediate program management responsibility for the FBI's analytical functions and produced, for the first time, a comprehensive strategy for the entire analytical arena. The Intelligence Analysts at the FBI are key players in achieving the FBI's comprehensive intelligence strategy. (U)

- The OI issued supplemental performance expectation guidance for all Intelligence Analysts, specifying expectations for the reports officer, operations specialist, and all-source analyst work roles. This communication was intended not only to inform analysts as to the expectations, but also to keep supervisors informed as to the proper utilization of the Intelligence Analyst position. The OI has instructed all FBI field offices that Intelligence Analysts must report through the Field Intelligence Group chain-of-command. (U)
- The OI assumed administrative control for all Intelligence Analysts on February 1, 2004. The OI is responsible for establishing and executing standards for recruiting, hiring, training, and developing the FBI's intelligence analytic workforce, as well as for ensuring that they are assigned to operational and field divisions based on intelligence priorities. Operational and field divisions are responsible for day-to-day supervision of Intelligence Analysts and for adhering to standards for analyst development established by the OI. (U)
- This new management model was implemented by placing the section chiefs at Headquarters currently performing intelligence functions under the operational control of the OI. Those section chiefs are rated by the appropriate official in OI and reviewed by the Headquarters investigative division into which they are integrated. (U)

Recommendation No. 3: Require greater coordination and consultation between the operational and analytical units. (U)

Response: The FBI agrees that an examination of the events surrounding the September 11 attacks showed a need for improvement in the coordination between operations and analytic units. We believe coordination and consultation has dramatically improved. Consistent with the Director's May 2002 announcement of the FBI Strategic Focus, the Counterterrorism Division was reorganized to implement a threat-team approach to better align the FBI's efforts to prevent terrorism. The revised approach moves away from a traditional hierarchical structure and separation between analytic and operational functions and employs matrix-management concepts used in successful businesses and private organizations and in government agencies. (U)

The goal of the reorganization was the implementation of an organizational structure and concept of operations that empowers and enables the FBI to achieve the priority of protecting the United States from terrorist attack by facilitating the flow of

[REDACTED]

information between operational units and their analytic counterparts. The FBI categorizes the current threat as follows: Radical Fundamentalists, Global Extremists, and Domestic Terrorists. Additionally, a cross-cutting threat in each of these areas is the terrorist acquisition of weapons of mass destruction (WMD) and the misuse of U.S. and international monetary rules and procedures. (U)

Using this threat-based framework, the FBI structured the operations of the CTD along a threat-team concept that organized the bulk of its investigative, financing, reports and requirements, and analytical resources into three threat teams. The components of each threat team are co-located to facilitate day-to-day interactions and create synergy between the investigative and intelligence disciplines. The CTD Assistant Director and Deputy Assistant Directors (DADs) jointly identify the investigative and analytic priorities, establish integrated operational and analytical objectives, and allocate CTD resources for each team based on those priorities and objectives. The operational strategies agreed upon for each threat team have been disseminated to all FBI field offices where they will guide field operational activities. The components of each threat team are co-located to facilitate day-to-day interactions and create synergy between the investigative and intelligence disciplines. (U)

The Office of Intelligence, meanwhile, has established principles within the Bureau that information belongs to the Bureau rather than a single field office or headquarter component and will be shared with all those with a legitimate need-to-know. The Office of Intelligence is also working with the Information Resources Division to develop the systems that will facilitate information sharing. (U)

Since the September 11 attacks, the FBI's Office of Intelligence has published a Concept of Operations for Intelligence Production and Use. This publication guides the FBI in the coordination of intelligence production. In general, the role of the operations components center on commenting on the accuracy of facts and the protection to be afforded for sources and methods. The Executive Assistant Director for Intelligence is the final arbiter in disagreements between operations and intelligence components in the production and dissemination of intelligence products. (U)

The FBI has put into place a number of other mechanisms that have vastly improved coordination between operations and analytic components. These include: (U)

- Twice daily intelligence and operations briefings chaired by the Director and attended by executives, lower-level managers, and line analysts from both the operations and intelligence components of the investigative divisions, as well as the Executive Assistant Director for Intelligence (EAD-I) and other OI managers. Coordination issues are discussed and directions are given for both operations and intelligence issues in connection with the priority threats and important investigations. (U)
- A daily Intelligence Production Board (IPB) was established in August 2003. The IPB meets daily and is chaired by the EAD-I. Representatives include senior

[REDACTED]

managers, unit-level managers, and line analysts from the intelligence components of all investigative divisions. Coordination issues and processes are discussed and resolved in these meetings in accordance with direction provided by the EAD-I. (U)

- The Director has designated the EAD-I as the FBI's chief policy official for Intelligence and Information Sharing. In this capacity, the EAD-I has policy authority to ensure the coordination recommended does indeed take place, and she has instituted a number of processes that have significantly improved coordination and consultation between operations and analytic units. (U)

B. Recommendations related to the FISA process: (U)

Recommendation No. 4: Ensure adequate training of FBI employees involved in the FISA process and counterterrorism matters. (U)

Response: The FBI is in agreement with the OIG's recommendation to ensure adequate training to employees involved in the FISA process and counterterrorism matters and has developed a program to address these issues. The Counterterrorism Division (CTD) has made tremendous progress in developing a training program that enhances the FBI's ability to conduct counterterrorism investigations that result in the prosecution of terrorists, disruption of terrorist organizations and support networks, and has led to an increase in the overall contribution of intelligence to the U.S. Intelligence Community and to senior policy makers in government. Training focuses on all aspects of the FBI's response to the threat of terrorism, both domestically and abroad, which includes international terrorist groups and/or countries of interest, domestic terrorism, weapons of mass destruction, terrorist financing operations, Foreign Intelligence Surveillance Act, National Security Guidelines, Patriot Act, source development, interview and interrogation techniques, rapid deployment, and digital and electronic exploitation. The CTD has developed this training through the identification of subject matter experts from within the FBI, other Government Agencies and private contractors. CTD has offered this training to FBI Special Agents and Analysts from both the field and headquarters as well as to law enforcement personnel assigned to the Joint Terrorism Task Forces (JTTF) throughout the country. CTD has contributed significantly to the courses developed by the College of Analytical Studies and the Central Intelligence Agency University for FBI Analysts. These courses aim to improve and enhance analytical capability to quickly ascertain the reliability, implications, and details of terrorist threats, and how threat-related information is disseminated to local, state, and federal agencies. (U)

CTD's primary focus is to address the most immediate training needs of the FBI's workforce. CTD has been working with the Training Division, Office of Training Development, to create curricula which addresses the needs of Agents, Analysts and Task Force Officers assigned to counterterrorism related matters. This curriculum based approach begins with a basic understanding of the foundation of both domestic and international terrorism and expands to a specific approach to counterterrorism investigations and implementation of the CT investigative strategy. In-service training

being conducted on a regular basis include: International Terrorism Basic Operations, International Terrorism Source Development, and Interview and Interrogation of Islamic Extremists. These training curricula are being developed to meet the needs of the FBI's ever changing counterterrorism mission. (U)

CTD has developed the course, "Counterterrorism: A Strategic and Tactical Approach", to address the overwhelming demand for training of state and local law enforcement officers engaged in counterterrorism related investigations through the JTTF. The core content of this training emphasizes an understanding of administrative and operational requirements in conducting terrorism investigations and operations. Course participants are briefed on a variety of international terrorist organizations; Middle East culture and mind set; and are exposed to concepts involving assessment; recruitment and handling of sources; surveillance methodology; interview/interrogation problems; techniques inherent in international terrorism matters; and case management. This course is presented regionally and provides the law enforcement officers, assigned to work on the JTTF, a better understanding of their vital role in the FBI's counterterrorism mission. Twenty five iterations of this course are planned for this year. (U)

Throughout FY03, CTD participated in designing a new approach to teaching New Agents during their four months of New Agent Training (NAT) at the FBI Academy. In late December 2002, a plan was designed to incorporate a counterterrorism (CT) and counterintelligence (CI) instructional block into the NAT to include 110 hours of CT and CI investigative curriculum. The new instructional block is an approach to investigative training which uses a Middle Eastern Criminal Enterprise (MECE) as a "thread" through the entire session of New Agent Training. The new CT and CI instructional block begins with "basic investigative techniques" and culminates in "advance investigative techniques." Each basic and advanced instructional block incorporates informant/cooperative witness/asset development as well as financial investigative techniques. (U)

Conferences that have been coordinated by CTD have targeted SACs, ASACs, SSAs, SAs, Analysts and JTTF Officers and have included Suicide Bomber Awareness, Working Together in Counterterrorism (FBI/CIA coordination), Terrorist Financing, Domestic Terrorism, Weapons of Mass Destruction, JTTF Annual Conference, and Special Event Management. Individual course content is specifically designed to address and meet the needs of a group's activities. Additional conferences are being scheduled to address recurring issues on animal rights, eco-terrorism, black separatists, domestic terrorism fugitives and international terrorist groups of interest such as Hamas and Al Qa'ida. CTD continues to support counterterrorism international training through the International Law Enforcement Academies (ILEA) and provides instruction by the Terrorist Financing Operations Section to the FBI's law enforcement partners world wide. (U)

The FBI's Office of Training and Development, in coordination with the Counterintelligence Division, Counterterrorism Division, and the National Security Law Branch (NSLB), Office of the General Counsel (OGC), has prepared and disseminated

Bureau-wide a FISA/Foreign Intelligence/Counterintelligence/Counterterrorism interactive "Distance Learning Program" for New Agents and all other FBI personnel assigned FCI/IT responsibilities. The course is entitled "FISA and Information Sharing: Their Impact on Investigations" and covers the following topics: Handling Classified Information; Sharing Investigative Information with the Intelligence Community; FISA Requirements and Process; and Sharing Intelligence with Prosecutors as per the March 6, 2002 Procedures. The course provides the user with a foundation on information sharing and its impact on investigations, the handling and safeguarding of classified material, and the FISA administrative process. All agents and analysts working on counterterrorism or counterintelligence investigations are required to take this distance learning course. It is accessible to all employees through the Virtual Academy, the FBI's Learning Management System. The CTD and the Office of Training and Development have also worked with the FBI's Virtual Academy program to develop an online content addressing the Patriot Act. (U)

In addition to the distance learning course, each of the 56 field divisions have conducted 2-days of "hands-on" FISA training. Instructional teams are appointed by the cognizant Assistant Special Agent in Charge (ASAC) and consist of an Assistant United States Attorney (AUSA), the Chief Division Counsel (CDC), a squad supervisor, and a Central Intelligence Agency (CIA) representative. Where possible, Office of Intelligence Policy and Review (OIPR), Department of Justice (DOJ) and FBI Headquarters personnel supplemented the instructional teams. The two-day curriculum covered the entire FISA process, including the initiation of FISA requests, minimization procedures, and the renewal process. These training sessions began in July, 2003, and continued through November 2003. (U)

Additionally, NSLB assigned two lawyers to support the Counterterrorism Division's National Security Programs Operational Training Unit (OTU) at the FBI Academy. OTU has expanded all New Agent training to include Foreign Counterintelligence and Counterterrorism instruction. That training is provided by OTU and NSLB personnel. (U)

NSLB also conducts joint-training with OIPR, DOJ, in selected field divisions at least once a month. In addition to six-hours of classroom instruction, several days are spent reviewing current and closed FISA cases with the assigned case agents and their supervisors. (U)

NSLB further provides FISA instruction for all Foreign Counterintelligence(FCI)/Counterintelligence (CI)/International Terrorism (IT) In-Service classes conducted at the FBI Academy. This training is conducted for more experienced FBI personnel (including ASACs, Chief Division Counsel, Special Agents, Intelligence Operations Specialists, Intelligence Research Specialists and other support personnel) who are now assigned FCI/CI/IT matters, and for personnel who are transitioning to those assignments. (U)

NSLB also provides FISA instruction to all FBIHQ operational units as additional FCI/CI/IT resources are assigned. NSLB has a newly-created National Security Policy

[REDACTED]

and Training Law Unit which, when fully-staffed, will assume broad training responsibilities for both FBIHQ and field division training in FISA and related matters. (U)

The CTD and the FBI's Office of General Counsel, National Security Law Branch, have worked to provide national security training to field Supervisors and ASACs at Department of Justice National Security Training Conferences held at the Department of Justice's National Advocacy Center. The NSLB assigned several attorneys as instructors to support the conferences which were conducted at the National Advocacy Center (NAC), DOJ, in Columbia, SC. The conferences were four days in length. This conference was developed to address the overwhelming concern regarding revisions to the National Security Investigative Guidelines and implementation of the Foreign Intelligence Surveillance Act (FISA). The first conference was held beginning on May 6, 2003. A total of six such conferences were conducted at the NAC during the summer months, and two conferences were held at Fort Belvoir, Virginia in September 2003. The attendees were SACs, Chief Division Counsel, Special Agents, Assistant United States Attorneys, and the attorneys assigned to the Office of Intelligence Policy and Review, DOJ, who were also providing instruction. The curriculum included instruction on the mission and organization of the Intelligence Community, an overview of the Foreign Intelligence Surveillance Act, information sharing, coordination between intelligence and law enforcement components, foreign intelligence and counterintelligence collection tools, the use of FISA information in support of criminal litigation, and practical and tactical decision-making. The conferences also included a day-long, problem-solving exercise, conducted in individual "breakout" sections, to reinforce the teaching objectives of the conference. (U)

The CTD also held a national security conference with the DOJ to train both Agents and Analysts on information sharing and coordination between the Intelligence Community and law enforcement; FISA; foreign intelligence and foreign counterintelligence investigations and collection tools; and the Patriot Act. Based on the success of both conferences, CTD implemented and developed a regional training course to guide all 56 Field Divisions on the Attorney General Guidelines for National Security Investigations and the FISA process. (U)

The Counterintelligence Law Unit in NSLB routinely participates in country-specific conferences that Counterintelligence Division units sponsor (usually on a yearly basis). The topics taught by NSLB include the National Security Guidelines and the FISA process. (U)

Before 09/11, NSLB (then the National Security Law Unit) provided extensive training at FBI conferences held annually for Chief Division Counsel (FBI Agent attorneys in the field divisions), including one such session which was funded by the Counterterrorism Section and devoted entirely to intelligence law issues. Additionally, NSLU provided intelligence law training for Chief Division Counsel at three regional training conferences in 1996 and 1997 which focused entirely on intelligence law issues.

[REDACTED]

NSLU also routinely provided intelligence law training at conferences sponsored by the Counterterrorism Section. (U)

NSLB also provides FISA training and guidance via periodic communications disseminated to all divisions: e.g., NSLB guidance entitled "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI" which was disseminated to all field divisions in November 2002. (U)

NSLB also maintains the OGC Intranet (available to HQ and all field divisions). Recent instruction included specific guidance on information sharing. The NSLB website also features an on-line, downloadable "brochure" entitled "How Do I Get a FISA?" (U)

With regard to FY04 training, CTD will continue to develop and implement training and conferences for Agents, Analysts, JTTF members, and state and local law enforcement. Furthermore, we are in the developmental stages of introducing, with the Office of Intelligence, an Analyst Handbook to further the mission of CTD and introducing new curriculum to train Reports Officers (RO). The Reports Tradecraft course provides the foundation for new ROs assigned to counterterrorism matters in which they will be trained on various intelligence collection management topics to include the FBI Intelligence Collection Cycle; identifying intelligence; dissemination of intelligence while protecting sources, methods and investigations; and writing intelligence information reports. (U)


CTD has developed a Counterterrorism Training Track to address the most immediate educational needs of Agents, Analysts, and JTTF Officers assigned to counterterrorism related matters, starting with a basic understanding of terrorist operations and moving on to intermediate and more advanced levels. (U)

Specific courses designed for the Basic level of training for Agents, Analysts, and JTTF Officers include: (U)

- International Terrorism Basic Operations – approximately 850 trained. (U)
- International Terrorism Source Development – approximately 300 trained. (U)
- Counterterrorism: A Strategic and Tactical Approach- approximately 210 plus 50 instructors trained. (U)
- Domestic Terrorism – approximately 39 trained. (U)
- Middle Eastern Culture/ISLAM 101 – online course (U)
- CT Training for State and Local Law Enforcement – 130 Agents trained as instructors for 26,880 law enforcement officers.(U)
- The College of Analytical Studies offers a series of courses for analysts that support the CT mission - approximately 250 trained. (U)

Courses designed for the intermediate level include: (U)

- IT Interview and Interrogation – new intermediate course for summer 2004 for 40 agents.(U)

- 
- Specialty topics including courses on the Arabian Peninsula and Hamas – approximately 100 trained. (U)
 - CTD works in collaboration with the CIA University offering specialty courses mainly focused on WMD issues – approximately 22 trained. (U)
 - Digital and Electronic Evidence Exploitation – approximately 80 trained. (U)
 - Internet and Email Communications Investigation – approximately 40 trained. (U)
 - Suicide Bomber Awareness Training – approximately 320 trained. (U)

Courses designed for the advanced level include: (U)

- Interview and Interrogation Techniques- 19 agents trained at the advanced level in Israel. (U)
- Development and Handling of Islamic Extremist Sources – 39 agents trained at the advanced level. (U)

The FBI's Senior Executive Service personnel are going through an executive development program that was created in partnership with the Kellogg School of Management, one of the country's leading business schools. In an intensive one-week course, FBI executives receive guidance on managing change, with a particular focus on the FBI's transition to new intelligence, investigative, and case management processes. As of February 13, 2004, 260 FBI executive managers have completed the training, including 12 Assistant Directors and 54 SACs. (U)

The following chart depicts the Counterterrorism Division projected training for FY2005:

COUNTERTERRORISM TRAINING STATUS FOR FY2005

CORE COURSES	TARGET AUDIENCE	LEVEL	DURATION	PROJECTED NEEDS
ME Culture Online	All Agents, Analysts, JTTF Members	BASIC	3-4 Hours	Imminent Launch Eventually add Intermediate level Use as model for Online
IT Basic Operations	50 Agents Analysts JTTF Members	BASIC	Every other Month for 5 days	Revise Goals/Objectives/Curricula Align with Competencies
JTTF Regional CT: A Strategic & Tactical Approach	35 Agents Analysts JTTF Members	BASIC	Once/Month for 5 days	Curriculum Update Ramp up to Intermediate Level Instructor Development Ongoing Evaluation/ Align with Competencies
IT Source Development Seminar	35 Agents Analysts JTTF Members	BASIC / Intermediate	Once/month for 3 days	Modify once Interview/Interrogation begins. Align with Competencies
Interview & Interrogation	20 Agents	Intermediate	Once/quarter For 5 days	Two Pilots offered in July and August 2004 Evaluation/Modify Align with Competencies
Interview & Interrogation	10 Agents (highly selective)	Advanced (including Israeli)	Twice per Year For 10 days	First Pilot offered FY 2005 Align with Competencies Status of Israeli training Ongoing Course Develop.
Specialty Groups Seminars: Hamas Al Qaeda Hizballah	35 Agents Analysts JTTF Members	Intermediate To Advanced	As Needed Basis for 2.5 days	Align with Competencies

Future Courses in Development:

- Overseas Deployment – Survival Training for Overseas Deployments in hostile environments (U)
- Analysts Training – Support Reports Officer Training at least once per quarter/2.5 days (U)
- ASAC/SSA Training – FBI/CIA Partnership, Specific Topics, Operations and Management, Guest Speakers for HQs once/month. (U)

- Online Courses – Identify which course information adapts easily to online Virtual Academy sponsored by the Training Division. (U)
- WMD and other specific International Terrorist Group Counterterrorism Training (U)

Recommendation No. 5: FBI Attorneys should be better integrated into counterterrorism investigations. (U)

FBI Response: After 9/11, the National Security Law Branch (NSLB) was restructured so as to mirror the operational structure of FBI Headquarters. Reflecting the operational division between the Counterterrorism Division (CTD), the Counterintelligence Division (CD), and the Cyber Division, three units were established within NSLB – two to handle counterterrorism matters (Counterterrorism Law Units (CTLU) I and II), and one unit to handle counterintelligence and cyber matters (Counterintelligence Law Unit (CILU)). (A fourth unit has recently been established to focus upon policy and training issues.) Within each of the three operationally-focused NSLB units, the attorneys are assigned to particular units or sections within CTD, CD or Cyber. Further, with regard to International Terrorism Sections I and II of CTD, NSLB has assigned two attorneys to be co-located in client space.(U)

Thus, with the assignment of an attorney to each of the operational units or sections, there is routine contact between agent, analyst and attorney on legal issues that arise. With regard to review of FISAs, NSLB attorneys have specific and focused knowledge of the targets for which their unit or section is seeking to initiate or renew coverage. At the point of initiation, the attorney is responsible for reviewing and approving the initiation submitted to him by his client, the operational unit. Any subsequent issues concerning that FISA which come to the attention of the operational unit with responsibility for the package is then routed to the attorney assigned that unit. The long-term result of this arrangement is an increased familiarity between client and counsel, and an improved working relationship. A sense of trust and purpose develops between the parties which greatly increases the likelihood that legal assistance will in fact be sought when it is necessary, and it increases the effectiveness of the attorney in responding to requests for legal assistance. Furthermore, the historic knowledge that the attorney gains by being assigned to a particular unit also increases his effectiveness, inasmuch as he has both present and past familiarity not only with the particular investigation that is the subject of the legal request, but with related investigations and the subject matter in general. (U)

The creation of new units within NSLB which have specific responsibilities for CTD, CD and Cyber units and sections has also increased contact with the field. NSLB attorneys have the opportunity for increased interaction with the field agents who are handling the investigations that are being supervised by the substantive units to which the attorneys are assigned. Recognizing that it is often the field office that will have questions requiring an immediate response or information needed by the NSLB attorney, particularly if the issue is the sufficiency or completeness of a request for FISA initiation, the NSLB attorney and the field agents have refined their working relationship, whereby

[REDACTED]

the NSLB attorney knows whom to turn to get answers to his questions, and the field agents know whom to seek out in order to resolve legal issues. (U)

Additionally, in the near future, NSLB will be further integrated with the Counterterrorism Division operational units due to the planned move to new office space in Tysons Corner, Virginia. The FBI, CIA, DOJ, and other agencies of the U.S. Intelligence Community will be co-located for the first time in large numbers in a single facility. At present, a total of 20 NSLB attorneys are expected to move to the new facility in Virginia. We expect that this move will result in the total integration of NSLB attorneys into counterterrorism investigations. (U)

Recommendation No. 6: Ensure closer consultation between the FBI and OIPR, particularly on important or unusual cases. (U)

Response: The FBI is in agreement with OIG's recommendation to coordinate closer with OIPR, and has taken steps to ensure that this is accomplished. In mid 2003, the CTD's International Terrorism Operations Section I (ITOS I) initiated bi-weekly operational meetings with representatives from DOJ OIPR and DOJ CTS to ensure that all operational and administrative facets of (1) ongoing criminal prosecutions in the field and (2) ongoing intelligence operations coordinated through OIPR, were in sync. Attendees at the weekly meeting include the ITOS I Section Chief or Assistant Section Chief, each of the four ITOS I Unit Chiefs or their representatives, and representatives from CTS and OIPR. During the meeting all entities field and ask questions, resolving most issues in the room. Typical issues include the status of high-visibility investigations in the field, the status of pending requests with OIPR, and the status of DOJ requests of FBI Field Divisions on those issues under the program management of ITOS I. (U)

ITOS I representatives were also heavily involved in the writing of the FISA Tiering system which provides a vehicle for FBI/OIPR prioritization of FISA applications awaiting presentation to the FISC. In light of ITOS I's large percentage of overall USIC FISA applications, Section members hold a wealth of experience in FISA matters and were able to contribute significantly. (U)

In May, 2004 CTD ITOS I recommended and initiated hosting of a weekly meeting with OIPR strictly for discussion on the status of pending and active FISA applications. This meeting does not discuss operational issues and is held separate and distinct from the weekly operational meeting. As of June 2004, all FBI entities involved with presenting FISA applications to the FISC were in routine attendance and the ITOS I tracking system used internally for the section was modified and adopted for overall FBI use. At this meeting OIPR and the FBI balance the list of pending FISC applications through discussion of the last week's docket, any emergency FISAs taken to court but not yet included in any database, and FISA withdrawals. This combination of weekly meetings, the FISA Tier System, and the FISA Tracking System have resulted in closer coordination between the FBI and OIPR. (U)

In addition, there is regular and significant consultation between the FBI and the OIPR concerning issues that arise with regard to the initiation and renewal of Foreign

[REDACTED]

[REDACTED]

Intelligence Surveillance Court (FISC)-authorized electronic surveillance and physical search packages, Standard Minimization Procedures, interpretation of the FISA statute, and myriad other matters. More specifically, there are biweekly meetings between OIPR supervisors and National Security Law Branch (NSLB) supervisors, including the General Counsel, and the CIA. There are also biweekly meetings on FISA issues between OIPR, NSLB, and the Office of the Deputy Attorney General. Moreover, impromptu meetings between supervisors of OIPR and NSLB, as well as meetings between line attorneys, are held almost daily. At present, there is regular and routine dialogue between the FBI and OIPR, at all levels, on important and unusual cases. (U)

On April 5, 2004, the Attorney General directed OIPR and the FBI to implement certain changes in the FISA process. This included the assignment of five NSLB attorneys to begin full-time one-year assignments to the "International Terrorism Operations Section I FISA Task Force" at FBIHQ to address pending requests for FISA coverage. Additionally, a total of 10 more NSLB attorneys will be assigned (some have already begun the assignment) to work full-time on the FISA process within OIPR's chain of command and under OIPR supervision for a period of one year. This assignment of attorneys has been beneficial in further integrating FBI attorneys into counterterrorism operations (addressed in recommendation #5). Overall, NSLB believes that the assignment of FBI attorneys will not only alleviate immediate OIPR staffing shortages, but will also serve to strengthen closer working relations between the FBI and OIPR. (U)

C. Recommendations related to the FBI's interactions with the Intelligence Community: (U)

Recommendation No. 7: Ensure effective management of FBI detailees. (U)

The FBI is in agreement that the OIG's recommendation to provide effective management to the employees detailed to the CIA's Counter-Terrorism Center (CTC). The FBI's Counterterrorism Division currently has one SES level manager, three GS-15 Supervisors, six GS-14 Supervisors and three Intelligence Analysts detailed to five CIA departments, including the Current Action Staff. All the CTC detailees are supervised through both the FBI and CIA chain of command for the specific department they are detailed, with the SES manager being their ultimate rating official. Each detailee has been made aware of their duties and responsibilities within their specified area of operation and this has been documented accordingly. In addition, all CTC detailees assigned to the CTC meet daily with the SES manager, and the GS-15 Supervisors meet again in the afternoon with the SES manager to prepare for the DCI's evening briefing [REDACTED]

The FBI has determined that the current performance plans for the GS-15 Supervisor, GS-14 Supervisor and the Intelligence Analysts are sufficiently inclusive to adequately reflect the critical elements of the job being performed by the individual detailee. As stated above, the FBI SES manager detailed to CTC serves as the rating or reviewing official as appropriate. CIA manager input is also solicited for the annual Performance Appraisal and semi-annual Performance Update. It should be noted that the SES manager at CTC does not have direct report authority to those FBI employees

[REDACTED]

detailed to CIA-FINO. These detailees are supervised by the Terrorism Financing Operations Section (TFOS) within CTD. The SES manager does ensure, however, that these employees are included in all meetings and provides necessary guidance and support while they are detailed to FINO. [REDACTED]

Recommendation No. 8: Ensure FBI employees who interact with other intelligence agencies better understand their reporting processes. (U)

Response: The FBI agrees that FBI employees need a better understanding of the reporting processes and capabilities of other U.S. Intelligence Communities, and it has taken, and will continue to take, steps to achieve this understanding across the FBI. The FBI does believe, however, that U.S. Intelligence Community agencies interacting with the FBI have an obligation to independently ensure that the FBI is fully informed about their reporting streams and all of the available information that they possess about pressing threat issues and investigations. (U)

Since September 11, 2001, the FBI has established a number of procedures and guidance directives to instill a better understanding of U.S. Intelligence Community reporting processes. These include: (U)

- The EAD-I has informed the heads of all Field Offices that U.S. Intelligence Community personnel who operate jointly with FBI Agents and analysts in the field must operate under the chain of command of the Field Intelligence Group in each Field Office. In this way, FBI personnel who have developed an expertise in intelligence matters can most effectively interact with U.S. Intelligence Community personnel. The respective agencies will be intimately familiar with each other's reporting processes and other capabilities. (U)
- In addition, the training curriculums for both New Agents and Intelligence Analysts is being revised to improve the knowledge that FBI employees have about U.S. Intelligence Community agencies, their roles, capabilities, and basic processes. (U)
- The Office of Intelligence has posted a glossary of the various types of intelligence reports produced by the U.S. Intelligence Community on its FBI intranet website. (U)
- A senior CIA official has been detailed to the FBI's Counterterrorism Division to enhance the FBI's knowledge of CIA counterterrorism operations and improve coordination. This official attends the daily briefings described earlier, where he discusses key CIA reporting streams and coordinates reporting exchange between the two agencies. (U)

Recommendation No. 9: Provide guidance for how and when to document intelligence information received from informal briefings by other intelligence agencies. (U)

Response: The FBI has taken this recommendation under advisement in its continuing development of intelligence policies and procedures. We note, however, that at the time of the verbal briefings by the CIA on Mihdhar around the time of the millennium threat, FBI policies to record this information did exist. They permitted the recording of this information by the FBI employee(s) in an Electronic Communication (EC), classified appropriately, and directed to the relevant file(s). (U)

Recommendation No. 10: Ensure that the FBI's information technology systems allow FBI employees to more readily receive, use, and disseminate highly classified information. (U)

The FBI has a responsibility to the nation, IC, Federal, State and Local law enforcement to disseminate information and to do so is an inherent part of its mission. Sharing FBI information will be the rule; filtering the information will be the exception, where sharing is legally or procedurally unacceptable. The FBI will deliver its information through the systems the FBI and its customers and partners use. (U)

The FBI is connected to the rest of the U.S. Intelligence Community at the Top Secret (TS) Sensitive Compartmented Information (SCI) level via the new SCI Operational Network (SCION). The SCION project was initiated in September, 2001, and has met all schedule, budget and performance requirements. SCION connects to the Intelligence Community (Intelink) [REDACTED]

[REDACTED] SCION is the business tool for the FBI's Office of Intelligence, Counterterrorism (CT), and Counter Intelligence (CI) Divisions. It has enabled FBIHQ CT and CI personnel to perform their duties more efficiently and effectively. [REDACTED]

SCION is currently available to over 1000 users at FBI Headquarters, and the FBI has initiated a pilot deployment project to the following Field Offices: New York, Boston, and Kansas City. The plan is to deliver SCION to all FBI Field Offices, as funding becomes available. Limited access to Intelink from other Field Offices is available through the old FBI Intelligence Information System Network (IISNET). Most of the Field Offices have two workstations which have a connection to FBI headquarters. These workstations are inadequate and difficult to use, and they are located in small Secure Compartmented Information Facilities (SCIF) that are not in the agent or analyst work areas. An impediment to field expansion of SCION is the lack of SCIF space for the Field Intelligence Groups (FIGs) and the Joint Terrorism Task Forces (JTTFs) personnel. (U)

[REDACTED]

Access to the intelligence and homeland security communities at the SECRET level is provided via the Department of Defense SECRET Internet Protocol Router Network (SIPRNET) which provides the communications backbone to INTELINK-Secret. Our goal is to provide SIPRNET/INTELINK-Secret access through secure dynamic virtual private networks to all FBI workstations in the near future. Today you cannot directly access any external networks from the FBINET and only limited batch transactions through secure guards are permitted. The Anti-Drug Network (ADNET) rides the SIPRNET communications backbone and provides terminals and access as a vehicle for the domestic exchange of intelligence on anti-drug efforts. SIPRNET is also used to support the Terrorist Explosive Device Analysis Center, the National Virtual Translation Center, and the Foreign Terrorism Tracking Task Force. [REDACTED]

In the area of organizational message traffic for dissemination of official information and taskings to other agencies, the FBI has just implemented its new FBI Automated Messaging System (FAMS) which is based on the Defense Messaging System (DMS). The FBI is the first civilian agency to operate the classified DMS. FAMS will provide on-line message creation, review, and search capabilities to everyone connected to FBINET. FAMS gives us the capability to send and receive critical organizational message traffic to any of the 40,000+ addresses on DMS or Automated Digital Network (AUTODIN). The TS/SCI version of FAMS is currently in testing and will provide the same capability to everyone on SCION or IISNET by the end of this year. The FBI's implementation of the DMS will provide writer-to-reader secure e-mail to internal and external users. Within the government, DMS will replace AUTODIN and a diverse array of e-mail systems currently in use throughout the Department of Defense and Intelligence Agencies. In its final form, DMS will become the government's global secure e-mail system. It will provide certified interoperability of various commercially off the shelf software products and connect over 2 million civilian and military users. The system will permit multi-media attachments to messages and provide end-to-end security. (U)

In the area of connectivity for data products, the FBI is just beginning to implement our initial programs for data marts as part of the Intelligence Community System for Information Sharing (ICSIS). Current FBI intelligence products in the form of Intelligence bulletins, Intelligence Assessments, and IIRs are being published on FBI web sites connected to SIPRNET and JWICS. The first FBI TS/SCI IC Data Mart (ICDM) is currently in development and should be on line by the end of 2004. The FBI Chief Information Officer is also working with the Department of Justice on interfaces between ICSIS and the Law Enforcement Information Sharing initiative and with the FBI Criminal Justice Information Services (CJIS) Division to increase the sharing of intelligence related information from and to state and local officials. (U)

The FBI is currently deploying the SECRET versions of FAMS, which uses DMS and secure Outlook like e-mail for organizational messages, so that our analysts and reports officers can send and receive timely intelligence with other agencies in near real time. The FBI is also working on a digital production capability for IIRs using extended markup language (XML) that will interface with FAMS and support on-line digital

production of intelligence reports. The FBI is applying XML data standards and meta-data tagging to facilitate the exchange of information with the intelligence community. The FBI is also applying new security technology to deploy a Protection Level 3 Data Mart capability with discretionary access controls and Public Key Infrastructure certificates in support of closed Community of Interests which will permit secure sharing of our most sensitive data with trusted members of other agencies. The FBI is also investigating the use of secure one way transfers to move information between security domains and to permit all-source intelligence analysis. The use of next-generation, community High Assurance Guards is being planned to provide for the two way transfer on critical intelligence between security domains. Secure wireless connectivity and Virtual Private Networks are also being looked at to provide increased access to intelligence to deployed personnel. The FBI is also starting to use On-line, desktop collaboration tools such as Info Work Space which is the foundation for the Intelligence Community Collaboration Portal to increase intelligence collaboration. (U)

The FBI plans to use additional systems as the foundation for additional information sharing with the IC, Federal State and Local entities. (U)

The CJIS National Data Exchange (NDEx) has plans for developing a systems approach to the operation, and maintenance of several interconnected IT and supporting telecommunications systems including Law Enforcement On-line (LEO) and CJIS WAN. The NDEx is to be a repository of national indices and a pointer system for state/local/federal and inter-governmental law enforcement entities. The NDEx will also be a fusion point for the correlation of nationally-based criminal justice information with certain national security data. (U)

Law Enforcement On-Line provides web-based communications to the law enforcement community to exchange information, conduct on-line education programs, and participate in professional special interest and topically focused dialog. The system has been operational since 1995 and presently serving about 30,000 users. LEO has secure connectivity to the Regional Information Sharing Systems network (riss.net). The FBI Intelligence products are disseminated weekly via LEO to over 17,000 law enforcement agencies and to 60 federal agencies, and providing information about terrorism, criminal and cyber threats to patrol officers and other local law enforcement personnel who have direct daily contacts with the general public. The FBI plans to enhance LEO for robust, high-availability operation. The FBI will use the enhanced LEO as the primary channel for sensitive but unclassified communications with other federal, state and local agencies. LEO and the Department of Homeland Securities Joint Regional Information Exchange System (JRIES) will be interoperable. (U)

The Investigative Data Warehouse (IDW) is following a multiple-phased approach to quickly provide support to FBI investigators, and Task Force members in the form of a spirally-developed operational prototype system, the *Secure Counterterrorism Operational Prototype Environment* (SCOPE). The enterprise system which builds upon SCOPE is the IDW system; the full deployment of IDW is scheduled for December 2004. The IDW will

help meet the law enforcement and the IC need for rapid, secure, dependable indexed data and will provide data mining access to FBI investigative files. (U)

The Multi-agency Information Sharing Initiative is intended to enable Federal, state, and local law enforcement agencies to share regional investigative files and provide powerful tools for cross-file analyses. A proof-of-concept effort is underway in St. Louis; additional demonstration sites are being planned. The goal of the demonstrations is to (1) show the value of sharing investigative data which can be analyzed by modern software tools; and (2) help define technical and organizational approaches for regional shared systems. Final decisions about deployment of the MIS will be based on the results of the demonstrations and the department wide plan for law enforcement information sharing being developed by the Department of Justice. (U)

With the creation of the Office of Intelligence at the FBI, each FBI field office has established a Field Intelligence Group (FIG). It is the responsibility of these FIGS to manage, execute and maintain the FBI's intelligence functions within the FBI. FIG personnel have routine access to TS and SCI information so they will be able to receive, analyze, review and recommend sharing this information with entities within the FBI as well as our customers and partners within the Intelligence and Law enforcement communities. (U)

Recommendation No. 11: Ensure appropriate physical infrastructure in FBI field offices to handle highly classified information. (U)

The FBI agrees with the recommendation and has taken steps to address the issue. To address the Bureau's increased demand for access to Sensitive Compartmented Information (SCI) systems the following actions have been taken: (U)

- 1) Large SCIFs are being designed and incorporated into new FBI Facilities. This will allow field offices investigative and intelligence elements to be located in areas that are conducive to the free flow of intelligence and common access to highly classified information systems. (U)
- 2) In addition, ten (10) field offices, including the New York Field Office mentioned in the above finding, have been identified as those that are most in need of SCIF upgrades. Associated costs include construction costs and miscellaneous costs. Miscellaneous costs include Eagle phones (1 per person); secure phones (1 per 10 people); shredders (1 per 10 people); and secure fax machines (1 per 30 people). This information was provided in response to Questions for the Record which followed from the March 30, 2004 testimony of DADs Harrington and Ford concerning the counterterrorism budget for FY 2005. The construction of the SCIF upgrades is dependent on the FBI receiving the required funding. (U)
- 3) The FBI is currently implementing a plan to adhere to the National Security Agency mandate to have all STU instruments replaced with STEs by 2005

[REDACTED]

Recommendation No. 12: Improve dissemination of threat information. (U)

Response: The FBI agrees that, like other intelligence and law enforcement agencies, it needed to improve in every way possible the processes used to disseminate threat information. Since September 11, 2001, the FBI has issued clear guidance for the dissemination of threat information. Additional policy development and training initiatives are in progress to further strengthen the FBI's threat information dissemination processes. Below are the steps the FBI has taken: (U)

- As indicated earlier, the FBI's EAD-I, a senior Intelligence Community career professional, has established concepts of operations, policies, and procedures related to the dissemination, both internally and externally, of threat information. (U)
- In December 2003, an EC was distributed to all Field Offices and Legats, entitled, "Reporting Raw Intelligence." This EC provided guidance, reporting thresholds, and reporting procedures for raw intelligence derived from FBI investigations and intelligence collection, and emphasized threat information reporting and dissemination procedures. (U)
- The FBI has prepared and distributed standing and ad-hoc sets of intelligence requirements (intelligence collection and reporting guidance) for agency-wide use. These requirements are posted on the FBI intranet and available to all employees. The requirements provide strategically-developed and well-defined intelligence needs concerning the threat environment. The requirements framework and format includes detailed reporting thresholds, time frames, and reporting instructions, to include reporting formats and to what components the threat information should be reported. (U)
- The FBI has developed and implemented a two-week specialized training course for analysts and agents in reporting and disseminating raw intelligence. This course teaches the evaluation of collected intelligence for dissemination, as well as reporting and dissemination trade craft using the most up-to-date FBI business processes, formats, and policies. (U)
- The FBI is nearing completion of the development of a new web-based Intelligence Information Report (IIR) application, which will serve to vastly improve the efficiency and effectiveness of reporting and disseminating threat information. The new application will contain a single IIR format for use throughout all of the FBI's programs, and will have a number of advanced features, such as electronic approval, date and time stamping, work flow tracking, and standard dissemination lists. The application will be supported by a comprehensive IIR handbook which will be distributed throughout the FBI in June 2004. (U)

[REDACTED]

The National Threat Center Section (NTCS) is the Counterterrorism Division's (CTD) focal point for the receipt, preliminary analysis, and assignment for immediate action of all emerging International Terrorism (IT) and Domestic Terrorism (DT) threats. The NTCS coordinates these threats with several entities and agencies, to include the Terrorist Threat Integration Center (TTIC), Terrorist Screening Center (TSC) and the Foreign Terrorist Tracking Task Force (FTTTF). (U)

The NTCS is comprised of five units: CT Watch (CTW), Public Access Center Unit (PACU), Strategic Information Operations Center (SIOC), Terrorist Watch and Warning Unit (TWWU), and Threat Monitoring Unit (TMU). TMU and CTW are responsible for most interfacing with TTIC, TSC, and FTTTF. (U)

Information Sharing with the Terrorist Threat Integration Center

Threat Monitoring Unit

The mission of TMU is to support the FBI's role in defending the United States from the threat of terrorism by receiving, assessing, disseminating, and memorializing threat information and suspicious activity in conjunction with FBIHQ, FBI Field Offices, Legal Attaches, and the U.S. Intelligence Community (USIC). (U)

Each month, TMU receives approximately 1,000 threat and suspicious activity referrals from various federal, state and local government and law enforcement agencies. Each of these referrals, in the form of e-mail transmissions, electronic communications, or hard copy submissions, are reviewed and assessed by TMU Supervisory Special Agent personnel. TMU immediately insures the appropriate FBI substantive units, Joint Terrorism Task Force (JTTF) agencies, or other government agencies, are expeditiously apprized of the threat information, and makes a record of this threat information referral. Additionally, if baseline criteria are met, these threat and suspicious activity reports are assigned to Technical Information Specialists who insure the threat information is researched, summarized, fully addressed, and entered in the searchable TMU threats database. (U)

During fiscal year 2003, TMU received and assessed approximately 11,000 threat and suspicious activity referrals. TMU subsequently memorialized more than 2,700 individual threat and/or suspicious activity reports in the TMU database. TMU disseminated the threat and suspicious activity information to the organizations and entities that had oversight responsibility for individuals or property affected by the threat or incident. TMU routinely provides all threats meeting its baseline criteria to the Terrorism Reports and Requirements Section (TRRS) who disseminates the information in the form of an Intelligence Information Report (IIR), to multiple counterterrorism customers, including TTIC. Before the FBI became actively involved in the publication of IIRs, TMU had direct contact with TTIC on a daily basis. (U)

Over 300 individualized searches of the TMU threats database were requested of, and conducted by, TMU to facilitate threat trend analysis by FBI units, the Department of

[REDACTED]

Homeland Security, the National Infrastructure Protection Center, and other agencies of the USIC who are seeking to measure target vulnerability. Also, in 2003, over 200 individual threat items were submitted by TMU to TTIC for publication in the joint FBI/Central Intelligence Agency Threat Matrix. This threat information was then distributed to the President as well as multiple federal agencies. TMU also received requests for, and conducted, more than twenty specialized threat database searches for major events (i.e., Superbowl, World Series), and for significant dates such as those corresponding with religious celebrations. (U)

Counterterrorism Watch

All TTIC personnel with access to FBI internal e-mail have been granted proxy rights to the main CT Watch e-mail folder and the CT Watch Daily Log. Many new issues and updates are reported to CTW by e-mail. All actions taken, incoming telephone calls, faxes, teletypes and e-mails are documented, in detail, in the Daily Log. Through this unlimited, real-time access to both the e-mail and log, all information reported to CT Watch is also available to TTIC. Furthermore, a CTW analyst is physically assigned to TTIC where they serve in a liaison role, ensuring information is shared between the FBI and TTIC. Conversely, CTW personnel also have access to TTIC Online where TTIC records all new threat information and provides updates on current threat investigations. In the late summer to early fall of 2004, CTW will be relocated to a new building and, as such, will be physically collocated with TTIC. (U)

Information Sharing with the Terrorist Screening Center

The TSC initially receives an inquiry from a law enforcement agency subsequent to a Violent Gangs and Terrorist Organization File (VGTOF) record match. The TSC communicates with the inquiring law enforcement agency to provide direction and confirm a match on the subject(s). If a possible match is made, the TSC generates a report containing all pertinent biographical data and a checklist of any research conducted. The TSC then makes direct contact with the CTW via telephone and/or secure facsimile to provide the information regarding the possible match. (U)

Upon receipt of the telephonic notification from the TSC, an analyst from the CTW will review all identifying information regarding the possible terrorist subject and confirm any database searches already conducted by the TSC, such as National Criminal Instant Background Check, ACS and Tip-Off. If necessary, the analyst will initiate additional database searches to include: a more detailed ACS search, Telephone Applications, Integrated Intelligence Information Application, Treasury Enforcement Communication System, Watchlist, Department of State, Immigration and Naturalization Service, Transportation Security Administration, Bureau of Prisons, INTERPOL, and pertinent public databases such as ChoicePoint, AutoTrack, and LexisNexis. (U)

The CTW analyst provides a brief synopsis to a CTW Agent, who then coordinates reactive and investigative action with the field via the FBI JTTFs, Field/LEGAT Offices, FBI case agents, and/or FBI Airport Liaison Agents. The CTW

[REDACTED]

disseminates the information to all relevant agencies and coordinates final resolution directly with the JTTF. When confirmation regarding the final resolution is received from the JTTF, the CTW provides a summary of the encounter in the CTW/TSC Group Daily Logs. These TSC Group Daily Log entries contain specific details such as names, locations, identifiers, call-back numbers, and a description of how the matter was resolved. The log entries are read in real time by FBI personnel at the TSC in Crystal City, Virginia, and used to document a final resolution for the encounter and "close the loop." The TSC ultimately reports all pertinent investigative and/or intelligence information back to the respective agency that nominated the terrorist-related subject for inclusion into the VGTOF database (TTIC or FBI). (U)

Information Sharing with the Foreign Terrorist Tracking Task Force

A representative from the FTTTF has been assigned full-time to CTW. Additionally, under the new CTD organizational chart, FTTTF has been placed under the umbrella of the NTCS. This collocation of resources will facilitate the flow of information between the NTCS and FTTTF. (U)

D. Other Recommendations:

Recommendation No. 13: Evaluate the effectiveness of the rapid rotation of Supervisory Special Agents through the FBI Headquarters' Counterterrorism Program. (U)

Supervisory Special Agents (SSAs) assigned to the Counterterrorism Division follow the same career path and related promotional timetables established for all Agent supervisors assigned to FBI Headquarters (FBIHQ). First line supervisors in the field and at FBIHQ have on average served as investigators for 10.5 years prior to assuming their management positions. GS-14 SSAs currently serving at FBIHQ have on average 2.43 years in their FBIHQ SSA positions. FBIHQ SSAs are in fact required to complete at least two full years in their HQ assignment before their transfer to other assignments. Even then, far from being a prescheduled rotation, their movement to a field assignment requires that they successfully compete for assignments pursuant to the demanding requirements of a completely restructured selection system. (U)

Similar to other intelligence agencies, the FBI's growing cadre of experienced support intelligence analysts and other operations specialists provide a significant portion of the continuity of knowledge required to understand and effectively evaluate the emerging threats over the long term. However, it is not accurate from the perspective of the FBI to characterize a two-year commitment to an FBIHQ position as a "rapid rotation," implying that SSAs on these two-year assignments contribute at a less than optimum level to the FBI's counterterrorism mission due to their length of service. The intention of service at FBIHQ is to provide Bureau leaders, selected on the basis of their demonstrated achievements, with a series of uniquely intense, particularly demanding challenges. The assignments provide experiential opportunities on a national and global scale. First line managers, working with their more experienced superiors and supported

[REDACTED]

by a knowledgeable intelligence staff, play a vital role in the identification of operational priorities, development and implementation of agency-wide initiatives, the assessment of the effectiveness of those initiatives, and the preparation of proactive responses to address emerging trends. These FBIHQ SSAs subsequently utilize this gained knowledge and experience in the domestic field and overseas in furtherance of the FBI's mission. (U)

If the FBI is to foster the development of true leaders to enhance its management cadre, it is imperative that all first line and mid-level managers actively and fully avail themselves of the widest possible range of leadership challenges, most particularly those available in FBIHQ SSA positions. The FBI's Executive Development and Selection Program has sought to strike the appropriate balance between providing first line managers with a range of developmental opportunities, and thereby address leadership succession concerns, while still providing continuity in the management of priority programs and regularly reinvigorating those programs with the new perspective and approaches of new first line managers. (U)

Recommendation No. 14: Provide guidance on the type of information that agents should obtain for evaluating assets and for documenting the yearly check on assets. (U)

The FBI agrees with recommendation and has implemented policy to address the issue. Current policy requires agents to provide semi-annual or annual evaluations, depending on the type of asset being developed or operated. The NFIPM Section 27-26 establishes 12 points which must be addressed in each evaluation. Among the twelve points are: 1) accomplishments attributable to the asset, 2) a characterization statement of the asset, and 3) the amount of money paid to the asset. The annual evaluation is not intended to document the asset's bona fides. NFIPM Section 27-29 provides examples of tests that the handling agent might utilize to determine the asset's bona fides. Additional steps to validate the asset are conducted by the handling agent and are used to determine the asset's reliability and veracity of the information they provided. These areas of reporting lend themselves to the administrative facet of asset development and operation. (U)

Within one year of opening and every 18 months thereafter, the handling agent is required to submit a case agent assessment to FBIHQ. This assessment is a brief narrative based on the handler's observations of and interactions with the asset, and provides insight into an asset's motivation and control, beliefs, habits and any significant behavioral changes. This time table does not preclude the agent from submitting a revised case agent assessment in the interim if the asset's behavior changes significantly. Additionally, a revised version of the NFIPM section 27 is currently in the draft stage. The new NFIPM will include language that directs agents to notify their immediate supervisor if they identify a significant change in the asset. The SSA will then determine if the asset's behavioral change rises to a level which would require FBIHQ notification. (U)

[REDACTED]

[REDACTED]

In contrast, agents receive information from assets which, although administrative in nature, and depending on the information's bearing on the investigative program, may require followup. These areas of reporting lend themselves to the investigative facet of asset development and operation. Further, this facet of asset development and operation are dictated by the logical progression of the investigative process and cannot be limited to or defined in administrative policy. (U)

Recommendation No. 15: Improve the flow of intelligence information within the FBI and the dissemination of intelligence information to other intelligence agencies. (U)

The FBI has a responsibility to the nation, IC, Federal, State and Local law enforcement to disseminate information and to do so is an inherent part of its mission. Sharing FBI information will be the rule; filtering the information will be the exception, where sharing is legally or procedurally unacceptable. The FBI will deliver its information through the systems the FBI and its customers and partners use. (U)

The FBI is connected to the rest of the U.S. Intelligence Community at the Top Secret (TS) Sensitive Compartmented Information (SCI) level via the new SCI Operational Network (SCION). The SCION project was initiated in September, 2001, and has met all schedule, budget and performance requirements. SCION connects to the Intelligence Community (Intelink) [REDACTED]

[REDACTED] SCION is the business tool for the FBI's Office of Intelligence, Counterterrorism (CT), and Counter Intelligence (CI) Divisions. It has enabled FBIHQ CT and CI personnel to perform their duties more efficiently and effectively. [REDACTED]

SCION is currently available to over 1000 users at FBI Headquarters, and the FBI has initiated a pilot deployment project to the following Field Offices: New York, Boston, and Kansas City. The plan is to deliver SCION to all FBI Field Offices, as funding becomes available. Limited access to Intelink from other Field Offices is available through the old FBI Intelligence Information System Network (IISNET). Most of the Field Offices have two workstations which have a connection to FBI headquarters. These workstations are inadequate and difficult to use, and they are located in small Secure Compartmented Information Facilities (SCIF) that are not in the agent or analyst work areas. An impediment to field expansion of SCION is the lack of SCIF space for the Field Intelligence Groups (FIGs) and the Joint Terrorism Task Forces (JTTFs) personnel. (U)

Access to the intelligence and homeland security communities at the SECRET level is provided via the Department of Defense SECRET Internet Protocol Router Network (SIPRNET) which provides the communications backbone to INTELINK-Secret. Our goal is to provide SIPRNET/INTELINK-Secret access through secure dynamic virtual private networks to all FBI workstations in the near future. Today you

[REDACTED]

cannot directly access any external networks from the FBINET and only limited batch transactions through secure guards are permitted. The Anti-Drug Network (ADNET) rides the SIPRNET communications backbone and provides terminals and access as a vehicle for the domestic exchange of intelligence on anti-drug efforts. SIPRNET is also used to support the Terrorist Explosive Device Analysis Center, the National Virtual Translation Center, and the Foreign Terrorism Tracking Task Force. [REDACTED]

In the area of organizational message traffic for dissemination of official information and taskings to other agencies, the FBI has just implemented its new FBI Automated Messaging System (FAMS) which is based on the Defense Messaging System (DMS). The FBI is the first civilian agency to operate the classified DMS. FAMS will provide on-line message creation, review, and search capabilities to everyone connected to FBINET. FAMS gives us the capability to send and receive critical organizational message traffic to any of the 40,000+ addresses on DMS or Automated Digital Network (AUTODIN). The TS/SCI version of FAMS is currently in testing and will provide the same capability to everyone on SCION or IISNET by the end of this year. The FBI's implementation of the DMS will provide writer-to-reader secure e-mail to internal and external users. Within the government, DMS will replace AUTODIN and a diverse array of e-mail systems currently in use throughout the Department of Defense and Intelligence Agencies. In its final form, DMS will become the government's global secure e-mail system. It will provide certified interoperability of various commercially off the shelf software products and connect over 2 million civilian and military users. The system will permit multi-media attachments to messages and provide end-to-end security. (U)

In the area of connectivity for data products, the FBI is just beginning to implement our initial programs for data marts as part of the Intelligence Community System for Information Sharing (ICSIS). Current FBI intelligence products in the form of Intelligence bulletins, Intelligence Assessments, and IIRs are being published on FBI web sites connected to SIPRNET and JWICS. The first FBI TS/SCI IC Data Mart (ICDM) is currently in development and should be on line by the end of 2004. The FBI Chief Information Officer is also working with the Department of Justice on interfaces between ICSIS and the Law Enforcement Information Sharing initiative and with the FBI Criminal Justice Information Services (CJIS) Division to increase the sharing of intelligence related information from and to state and local officials. (U)

The FBI is currently deploying the SECRET versions of FAMS, which uses DMS and secure Outlook like e-mail for organizational messages, so that our analysts and reports officers can send and receive timely intelligence with other agencies in near real time. The FBI is also working on a digital production capability for IIRs using extended markup language (XML) that will interface with FAMS and support on-line digital production of intelligence reports. The FBI is applying XML data standards and meta-data tagging to facilitate the exchange of information with the intelligence community. The FBI is also applying new security technology to deploy a Protection Level 3 Data Mart capability with discretionary access controls and Public Key Infrastructure certificates in support of closed Community of Interests which will permit secure sharing

[REDACTED]

of our most sensitive data with trusted members of other agencies. The FBI is also investigating the use of secure one way transfers to move information between security domains and to permit all-source intelligence analysis. The use of next-generation, community High Assurance Guards is being planned to provide for the two way transfer on critical intelligence between security domains. Secure wireless connectivity and Virtual Private Networks are also being looked at to provide increased access to intelligence to deployed personnel. The FBI is also starting to use On-line, desktop collaboration tools such as Info Work Space which is the foundation for the Intelligence Community Collaboration Portal to increase intelligence collaboration. (U)

The FBI plans to use additional systems as the foundation for additional information sharing with the IC, Federal State and Local entities. (U)

The CJIS National Data Exchange (NDEx) has plans for developing a systems approach to the operation, and maintenance of several interconnected IT and supporting telecommunications systems including Law Enforcement On-line (LEO) and CJIS WAN. The NDEx is to be a repository of national indices and a pointer system for state/local/federal and inter-governmental law enforcement entities. The NDEx will also be a fusion point for the correlation of nationally-based criminal justice information with certain national security data. (U)

Law Enforcement On-Line provides web-based communications to the law enforcement community to exchange information, conduct on-line education programs, and participate in professional special interest and topically focused dialog. The system has been operational since 1995 and presently serving about 30,000 users. LEO has secure connectivity to the Regional Information Sharing Systems network (riss.net). The FBI Intelligence products are disseminated weekly via LEO to over 17,000 law enforcement agencies and to 60 federal agencies, and providing information about terrorism, criminal and cyber threats to patrol officers and other local law enforcement personnel who have direct daily contacts with the general public. The FBI plans to enhance LEO for robust, high-availability operation. The FBI will use the enhanced LEO as the primary channel for sensitive but unclassified communications with other federal, state and local agencies. LEO and the Department of Homeland Securities Joint Regional Information Exchange System (JRIES) will be interoperable. (U)

The Investigative Data Warehouse (IDW) is following a multiple-phased approach to quickly provide support to FBI investigators, and Task Force members in the form of a spirally-developed operational prototype system, the *Secure Counterterrorism Operational Prototype Environment* (SCOPE). The enterprise system which builds upon SCOPE is the IDW system; the full deployment of IDW is scheduled for December 2004. The IDW will help meet the law enforcement and the IC need for rapid, secure, dependable indexed data and will provide data mining access to FBI investigative files. (U)

The Multi-agency Information Sharing Initiative is intended to enable Federal, state, and local law enforcement agencies to share regional investigative files and provide powerful tools for cross-file analyses. A proof-of-concept effort is underway in St. Louis; additional

[REDACTED]

[REDACTED]

demonstration sites are being planned. The goal of the demonstrations is to (1) show the value of sharing investigative data which can be analyzed by modern software tools; and (2) help define technical and organizational approaches for regional shared systems. Final decisions about deployment of the MIS will be based on the results of the demonstrations and the department wide plan for law enforcement information sharing being developed by the Department of Justice. (U)

With the creation of the Office of Intelligence at the FBI, each FBI field office has established a Field Intelligence Group (FIG). It is the responsibility of these FIGS to manage, execute and maintain the FBI's intelligence functions within the FBI. FIG personnel have routine access to TS and SCI information so they will be able to receive, analyze, review and recommend sharing this information with entities within the FBI as well as our customers and partners within the Intelligence and Law enforcement communities. (U)

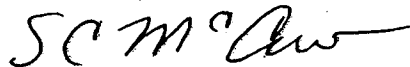
Recommendation No. 16: Ensure that field offices allocate resources consistent with FBI priorities.

The FBI agrees with the general concept that the recommendation is based upon and has in fact instructed each field office to address higher priority matters before lower ones. The Director has instructed the field offices to use whatever resources are necessary to handle all Counterterrorism leads. However, it must be pointed out that the level of resources allocated to each priority is not based upon the relative rank of the priority but upon the level and significance of the threat in each priority area and the extent to which the FBI has sole jurisdiction over the matter. Thus, to determine that the appropriate level of resources is allocated to each priority, a simple formula cannot be used. A detailed analysis of the threat and workload in every FBI division must be conducted.

This analysis of the threat and workload is conducted by each FBI program as part of the FBI's resource allocation process. In addition, the FBI has developed and implemented semi-annual program reviews to ensure each field office is appropriately addressing the FBI and the national program priorities. Headquarter's program managers are required to review each office's program review submission and make appropriate management decisions. In addition, the FBI's Inspection Division will use the semi-annual review submissions as a source document of conducting the field office

inspections. If field offices are not addressing priority matters appropriately, the Inspection Division will write a "finding" and require a corrective action be taken. The Inspection Division will also review the actions of the national program manager to ensure that appropriate instruction and actions were taken.

Sincerely yours,



Steven C. McCraw
Assistant Director
Inspection Division

Enclosure